CLAUSE J.1, ATTACHMENT A

PERFORMANCE WORK STATEMENT

FOR

HEADQUARTERS INFORMATION TECHNOLOGY SUPPORT SERVICES (HITSS)

NNH11351229R

APRIL 8, 2011

NASA Headquarters

Information Technology and Communications Division (ITCD)

INDEX

Table of Contents

1.0 Introduction

The Chief Information Officer in the NASA Headquarters Information Technology and Communications Division (ITCD) is providing this Performance Work Statement (PWS) on behalf of NASA Headquarters. The purpose of this Performance Work Statement is to provide a framework for information technology support services to NASA Headquarters.

The mission of NASA Headquarters is to provide overall guidance and direction to the Agency. Headquarters is organized into four Mission Directorates (Aeronautics, Exploration Systems, Science, and Space Operations), the Mission Support Directorate, and several Administrator Staff Offices, including the Chief Financial Officer, Chief Information Officer, Chief Technologist, and Chief Engineer.

The mission of ITCD is to support NASA Headquarters (HQ) by providing quality IT services, enabling HQ customers to accomplish NASA's mission. ITCD's vision is to deliver reliable, innovative and respected IT solutions. Its key organizational values are integrity, responsibility, helpfulness, effectiveness, and collaboration. As the Agency is moving forward with the NASA IT Infrastructure Integration Program (I^3P), collaboration is of special importance.

The HQ IT Support Services (HITSS) Contractor is expected to:

a. Provide expert advice and value-added guidance to Headquarters in developing cost effective solutions for its customer's IT requirements;

b. Provide an IT environment that fosters development of custom applications in a robust and evolving environment and takes full advantage of industry standards and emerging technologies;

c. Operate the NASA Headquarters data center environment in an efficient and effective manner;

d. Support IT requirements that utilize specialized IT skills and knowledge of technology trends to significantly increase user productivity and efficiency;

e. Provide excellent customer service for a variety of IT disciplines and functional areas;

f. Incorporate IT security in all aspects of the work to ensure protection of NASA Headquarters' data and systems;

g. Effectively collaborate with other Headquarters and Agency IT Contractors to provide seamless services to customers; and

h. Ensure that all IT activities meet all applicable Federal, OMB, OPM, Agency, and Headquarters requirements.

The specific support services required under this contract include: planning and management of information systems; life-cycle support for applications and information systems; operation of the NASA HQ Data Center; systems engineering and integration services; IT security; technology innovation and infusion; and customer support.

Not included within scope of this PWS are services provided through the NASA I^3P initiative and the NASA Shared Services Center (NSSC). The HITSS Contractor shall collaborate and integrate with the I^3P Contractors as well as the NSSC Contractor providing NASA-wide Enterprise Service Desk (ESD) and Enterprise Service Request System (ESRS) services. A high level view of the five I^3P acquisitions includes the following enterprise services:

- ACES (Agency Consolidated End-user Services): End-User Services – to include NASA desktops, laptops, cell phones, Personal Digital Assistants (PDAs), Agency-wide Active Directory, e-mail and calendaring functionality;
- NICS (NASA Integrated Communications Services): Communications Services – to include data, voice, video, LAN and WAN services;
- NEDC (NASA Enterprise Data Center): Data Center Services – to include application/data hosting and housing;
- WEST (Web Enterprise Service Technologies): Web Services – to include public-facing website hosting and applications; and,
- EAST (Enterprise Applications Service Technologies): Enterprise Applications Services – to include applications services associated with the NASA Enterprise Applications Competency Center and Agency-wide collaboration services including NASA's Identity, Credentialing, and Access Management (ICAM) in addition to new intranet environments and applications.

This PWS represents a comprehensive set of core requirements in the areas of program management, program-wide services, customer relationship management, application development and information management, NASA HQ Data Center support, systems engineering and integration, and IT security. Other related services may be required during the life of the contract to provide direct support to Mission Directorates and Mission Support organizations in the areas of dedicated system development and/or subject matter expert support. These other services will be ordered through the indefinite delivery, indefinite quantity provisions of the contract.

2.0 Program Management

Effective program management is the cornerstone of successful contract execution. The Contractor will be responsible and accountable for ensuring the quality and timeliness of products and services delivered under this contract. This requires technical expertise and the ability to establish technical credibility among HQ customers. However, good program management also includes, but is not limited to, the following characteristics:

- Leadership – The Contractor's program management team should lead its team by example toward the successful accomplishment of its mission, despite the problems that any program/project will encounter. Leadership implies more than managerial skills. It includes looking ahead to see the big picture, anticipating potential problems, resolving them as quickly as possible, and providing the environment that enables the team to be successful. Commitment to excellence and respect for team members and partners are strong elements of leadership.
- Communications – The Contractor is responsible for doing its part to facilitate productive communications among all parties, including the Government, customers, and other service providers. Open communications and transparency breeds trust and mutual respect, even if the news isn't always good news. Involving the right people in the conversations can lead to quicker problem solving and a stronger team.
- Managing Relationships – Building and maintaining effective relationships with stakeholders is critical to success of this program. Stakeholders include HQ management, customers, other NASA Centers, and other service providers that depend on services performed under this contract. Managing expectations is an important component of healthy relationships – don't over-promise or under-deliver.
- Teambuilding – A strong, integrated Government-Contractor team is supportive and proactive. Good program management includes strategies to keep the team together and working toward mutual goals.
- Institutional Support – Although technical expertise is important, a strong organization with access to resources for staffing and budgeting is a critical component of effective program management.

Other program management requirements specific to this contract include:

2.1 Online Documentation Environment for Metrics, Analysis and Deliverables (On DEMAnD)

Throughout the life of this contract, the Contractor shall leverage opportunities for collaboration and shall satisfy all stated deliverables and metrics that are identified throughout this PWS. The Government requires minimizing the submission of paper documents during this contract and maximizing the online discovery of and relationship between documentation, inventory assets, plans and analytical artifacts. To accomplish this, the Government expects the Contractor to establish, provide, and then continue to develop and enhance an online environment that achieves the following goals:

a. provides a secure site for Contractor and HQ personnel to collaborate in the execution of HITSS activities and to develop products. Content posted to the site shall include linkages to and between related deliverables and supporting artifacts, outage notifications, training documentation, technical documentation, security plans, baselined inventory, standard procedures, as-built drawings, processes, guidelines and DRDs (Data Requirements Documents);

b. leverages existent authoritative data sources such as Patchlink, server logs, network monitoring and configuration management databases (e.g. ROSA (Repository of Supported Applications), STACR (Subversion/Trac Application Code Repository)), procedural databases (e.g. SOPR (Standard Operating Procedures Repository)) and graph-based data aggregation systems (e.g. BIANCA (Business Impact Analysis for Network Computer Assets)). HQ currently has 212 SOPs in SOPR and uploads approximately 120 documents in to ROSA per month;

c. establishes technical approaches, procedures, standards and mechanisms to ingest new authoritative data sources in to the On DEMAnD service;

d. ensures visibility, at varying levels as appropriate, to project plans and management activities, including schedule, resources, milestones, and trending sufficient to discuss alternatives or priority tradeoffs;

e. contains current information as well as history of key areas to determine trending;

f. can be leveraged as the environment to ingest data from authoritative sources outside of HQ for the purpose of activity reporting (e.g. On Boarding);

g. manages service requests by utilizing on-line tools that enable users to initiate and track them through an online system, and integrates this system with the NSSC's Enterprise Service Desk and Enterprise Service Request System;

h. is accessible, at varying levels as appropriate, via web browsers to the Contracting Officer's Technical Representative (COTR), Contracting Officer (CO), ITCD Performance Monitors, Mission Directorate and Mission Support Task Managers, and other HQ personnel;

i. contains financial reporting, task order management, invoicing and similar business information from the contractor's business system;

j. provides ability to view documents and analysis and an option to download;

k. is searchable, sort and retrievable by relationships and/or by common attributes;

l. provides an index and explanations of variances for metrics falling outside the minimum standard; and

m. provides visibility into all aspects of technology updates including schedules for quarterly refresh, bi-annual technical infusion, prototypes, pilots, and plans.

DRD	Description	Frequency
DRD #1	Documentation environment of metrics, analytics and deliverables implementation plan and migration schedule.	Updated and available weekly during the first two months of contract start date; enhancements and additional content added monthly thereafter until established baseline schedule is met.

2.2 Contract Transition and Stabilization

The contract transition and stabilization period will be from contract award and continue for six months. There are several plans, reports and reviews the government requires during the first 6 months of the contract and theses activities shall be well coordinated, tightly integrated, and professionally implemented. The goals will be to provide uninterrupted services to our customers, continuous visibility in to the performance of transition activities, and continued improvement.

Technical performance incentives for the first six months of the contract will be focused on five overarching plans that are foundational to the success of contract transition and stabilization activities and the continued success for the duration of the contract. The plans are:

- Application Service Framework
- Application Service Roadmap and Implementation Plan
- Data Center Modernization Plan
- Legacy Application Disposition Plan
- Training Program and Outreach Plan

These plans along with a successful closure of actions from the ORR and with customer satisfaction surveys from key stakeholders will form the basis of the incentive fee available.

In support of contractor transition activities the contractor shall:

a. deliver a detailed integrated schedule depicting status for each of the discrete transition activities;

b. ensure uninterrupted service delivery from data center assets;

c. ensure uninterrupted IT security surveillance and services;

d. ensure software, hardware, application and similar maintenance and license agreements are covered and transitioned;

e. ensure application development activities are uninterrupted and that software development assets are transitioned to assure that development effort schedules are maintained;

f. ensure projects in development are transitioned in a manner where customer satisfaction will be maintained or improved;

g. ensure Operational Level Agreements (e.g. with the NASA Data Center, ACES, NSSC) and Task Orders are signed and in place;

h. ensure customer outreach and communication activities are maintained or improved; and

i. ensure DRDs and plans are delivered and available.

DRD	Description	Frequency
DRD #2	Transition plan and integrated schedule	Available at contract start date with significant weekly updates for the transition period up to Operational Readiness Review and acceptance.

Metric	Description	Performance Level to Achieve Fee
Metric #T&S-1	Completion of Actions from Operational Readiness Review (ORR). Outstanding actions from the ORR shall be completed within the required time period.	90% - 95% of the actions are completed by the due date.
Metric #T&S-3	Stakeholder Satisfaction with Transition and Stabilization. Stakeholder ratings from transition shall be no less than a “4” on a scale of 1-5 with “5” being the highest.	91%-94% meet the criteria.

2.3 Program Management Reports and Reviews

A goal for the ITCD and HITSS team is for management and staff to be aware of program/project status on a continuous basis facilitated by precise, accurate and timely reporting and reviews. In addition to face-to-face meetings, the Contractor shall provide and promote online postings of current knowledge products in an orderly and intuitive manner and minimize the need to generate and email products for distribution. The success of this service should minimize issues of versioning, multiple email attachments and enable meetings to focus more on details of status, issues, initiatives and opportunities. To support specific meeting requirements the Contractor shall:

a. provision scheduling, invitation lists, and accurate documentation of minutes and actions;
b. plan, operate and support daily operational status tag-up meetings to brief the team on previous day's issues/status and current day's plans, review of escalated Service Requests (SRs), status of critical operational issues;
c. plan, operate and support weekly Configuration Control Board (CCB) meetings to review Services Requests, Preliminary Design Reviews (PDR), Critical Design Reviews (CDR), and Operational Readiness Reviews (ORR) status, changes to the baseline, issues of cross-Contractor or cross-service support and similar CCB functions; and
d. plan, operate and support monthly program meetings, and other forums/reviews as required to ensure focus on specific issues requiring leadership attention and coordination such as project risk versus planned, priority adjustment requests and analysis, outstanding critical project or program issues.

DRD	Description	Frequency
DRD #3	Contract Status Meeting.	Monthly – no later than last week of the month.
DRD #4	Daily Tag Up Review.	Daily.

2.3.1 Plan Development

A plan gives the government and the Contractor a mechanism to achieve desired results. It must be fact-based, implementable, and sustainable. As such, all plans delivered shall:

a. align with an identified goal or goals that have previously been concurred in by the Government;
b. identify the required skills needed;
c. state that overall implementation can be accomplished within the estimated cost of the contract, or includes an estimated cost and basis of estimate (must provide both to successfully meet this element);
d. discuss technology maturity that can be supported within the current or projected NASA IT infrastructure;
e. include 5-10 quantifiable short-term objectives that will be accomplished over the succeeding six months (does not apply to the Application Service Framework); and
f. be delivered and available on or before the due date.

Metric	Description	Performance Level to Achieve Fee
Metric #T&S-2	Content of Selected Initial Plans. The following Initial Plans will include the required elements specified in the PWS and IFQAP: -Application Service Framework -Application Service Roadmap and Implementation Plan -Data Center Modernization Plan -Legacy Applications Disposition Plan -Training Program and Outreach Plan	86%-92% of the required elements are included.

2.3.2 Plan Updates

Plans are often subject to new requirements, new constraints, and new technology opportunities. To effectively manage our workload, all plans shall be kept up to date and the relative priorities of plans shall be reflected in a Program-wide integrated schedule. All plan updates shall:

a. be kept current reflecting changes within 48 hours of project scheduled updates and approved re-baselined activities;
b. be reflected to the second level milestone in a Program-wide integrated schedule to the second milestone level; and
c. adhere to the plan's objectives unless variances are approved.

Additionally, the five overarching plans shall:

d. align with an identified goal or goals that have previously been concurred in by the Government;
e. identify the required skills needed;
f. state that overall implementation can be accomplished within the estimated cost of the contract, or includes an estimated cost and basis of estimate (must provide both to successfully meet this element);
g. include specific actions taken during the past six months, and associated results, that definitively demonstrate that the objectives from the previous update or plan have been accomplished;
h. includes 5-10 quantifiable short-term objectives that will be accomplished over the succeeding six months; and
i. be delivered and available on or before the due date.

Metric	Description	Performance Level to Achieve Fee
Metric #1	Content of Selected Initial Plans Updates. Semi-annual updates to the following Plans will include the required elements specified in the PWS and IFQAP: -Application Service Framework -Application Service Roadmap and Implementation Plan -Data Center Modernization Plan -Legacy Applications Disposition Plan -Training Program and Outreach Plan	83%-95% of the required elements are included.
Metric #2	Accomplishment of Plan Objectives. All objectives identified in the semi-annual updates to the following plans will be met: -Application Service Roadmap and Implementation Plan -Data Center Modernization Plan -Legacy Applications Disposition Plan -Training Program and Outreach Plan	81%-92% of the objectives are completed.

2.4 Integrated Master Schedule

The Contractor shall develop and maintain an ITCD Integrated Master Schedule (IMS) of all ongoing and planned activities. The primary purpose of the ITCD IMS, for use by the Contractor and Government, is to provide a day-to-day tool for executing the HQ IT Program, tracking individual project technical and schedule status sufficiently to depict any significant risks and priority trade-offs. It also serves to strengthen the effectiveness of Contractor/Government communications, providing an early warning system of issues and concerns regarding critical projects. The Contractor shall:

a. when specified by the COTR, include those projects for which the Contractor is not primarily responsible;
b. create and maintain the IMS using a scheduling tool that utilizes features such as resource loading and project dependencies to facilitate accuracy in reprioritization scenarios;
c. enable alternate categorization views that group projects by strategic portfolio, by department, or resources;
d. provide secure web access to the IMS for NASA and Contractor project management leads;
e. use IMS briefings to ITCD staff, including progress assessments, identification of problems and workarounds, and a discussion of critical path activities and urgent priorities; and
f. provide schedule adherence data that summarizes schedule performance for all milestones to include reporting of project re-baselines with explanations.

DRD	Description	Frequency/Standard
DRD #5	Integrated Master Schedule with ability to drill down to supporting data, including resource loading.	Updated every 2 weeks from contract start date.
DRD #6	Project Schedule Adherence Report.	Monthly – no later than second week of the month.

Metric	Description	Performance Level to Achieve Fee
Metric #3	Adherence to Project Schedules. For all new Service Requests completed during the evaluation period, all end dates shall be met in accordance with the baseline schedule.	94% - 97% meet the criteria.

2.5 Project Management

Effective coordination and implementation of tasks is critical to the management of multiple activities of different sizes and types.   The Contractor shall implement project management tools and techniques for measuring progress and to achieve successful completion of project goals and objectives.

The Contractor ‘s activities shall be consistent with NASA Procedural Requirements (NPR) 7120.7, NASA Information Technology and Institutional Infrastructure Program and Project Management Requirements.

ITCD requires project management and tracking support for both internal and external projects. Internal projects are projects that are directly assigned to the Contractor by ITCD. An internal project could be a project sponsored by any HQ office and have a significant IT content. In providing this support, the Contractor shall use the governing documents specified by the requiring HQ office.

External projects are projects where the implementation lead is not the HITSS Contractor but where the Contractor shall be responsible for coordination, participation, or analysis. The Contractor shall provide comments and recommendations to HQ on project plans prepared by other Contractors and other NASA Centers, the Office of the CIO, or other Government agencies.

2.6 Risk Management

The Contractor shall identify and characterize IT-related risks, devising mitigation steps, and monitoring risks and mitigation activities on an ongoing basis. The Contractor shall provide support in drafting, for NASA consideration, risk management plans associated with IT investments. The requiring office will specify the format and overall requirements for the risk management activities, including the risk management plan. Those requirements shall be consistent with NASA policy concerning risk management. Currently, the following policy documents are relevant to this activity: NPR 8000.4 (Risk Management Procedural Requirements), Procurement Information Circular (PIC) 99-09 (Risk Management), NPR 7120.5 (NASA Program and Project Management Requirements and Processes), and NPR 2810.1 (Security of Information Technology).

2.7 Quality Assurance

The Contractor shall ensure the quality of Contractor provided products and services. The Contractor is responsible for assuring conformance of products to requirements, methods, and standards established by NASA, including verification and validation of products and services delivered under this contract. This shall include software assurance for all applications development activities. The Contractor shall provide, implement, and maintain a quality assurance process that includes plans and procedures to ensure that products and services delivered conform to contract requirements, reflect industry best practices, and are consistent with a lifecycle approach.

2.8 Logistics and Property Management

The Contractor shall maintain accurate asset records for all Government property for which the Contractor is responsible. This includes but is not limited to hardware, hardware maintenance, software, and software licenses. The records in the NASA property management application (e.g., N-PROP) shall be kept up to date. The Contractor shall conduct periodic inventories and adhere to the pertinent provisions and procedures of the most current NASA property management regulations. The contractor shall describe how they will meet the requirement and process for managing the onsite government property, government furnished equipment, and contractor acquired property. The Contractor shall, based on original quantity of inventory items, maintain lost property rate at 0.25% or less per year.

DRD	Description	Frequency
DRD #7	Logistics Management Plan.	One month after contract start date.

2.8.1 Support for Onsite Contractors

The Government shall provide office, desk and associated infrastructure to house up to 28 contractor employees for onsite support of the core requirements at NASA Headquarters. This includes, but is not limited to required onsite support in the following functional areas: Data Center Operations, Systems Engineering and Integration Test Facility, Video Teleconference Systems Support, User Resource Center, Computer Training Center, and Communications Security Support and Services (COMSEC). Additional office space may be made available for support of task orders under the IDIQ portion of the contract.

2.9 Contractor Training

The Contractor is responsible for all technical training of Contractor staff, unless otherwise directed by the Government. The Contractor shall provide technical staffing proficient in the tools and technologies utilized and supported under this contract. The Contractor may seek an exception when directed to implement a new technology and it is in the Government's best interest to utilize existing contract staff.

3.0 Program-wide Services

A goal of this contract is to provide an approach that will provide exceptional support across the program. Program-wide Services are those support activities that traverse all functional areas including; Enterprise Architecture, Concept of Operations, Problem and Incident Management, Change Management, Configuration Management, Safety, and Records Management. Customer Relationship Management and Service Delivery (section 4) are crosscutting for HITSS and extend to Agency Service Requests and Help Desk Management.

3.1 Enterprise Architecture

Enterprise Architecture (EA) is a comprehensive framework being used to manage and align NASA's Information Technology (IT) portfolio with its operational characteristics. The EA defines how information and technology will support the business operations and provide benefit for the business and illustrates an organization's core mission and each component critical to performing that mission. Critical components of the EA include:

- Guiding principles
- Organization structure
- Business processes
- Stakeholders
- Applications, data, and infrastructure
- Technologies upon which networks, applications and systems are built, and
- Security plans associated with these applications and systems**.**

3.1.1 HQ Enterprise Architecture Program

It is the mission of the NASA HQ Enterprise Architecture Program to engage stakeholders to better understand their mission requirements, and then apply architecture methods, tools, and products to produce higher fidelity information that improves their integrated planning, decision-making, and service delivery. The Contractor shall support NASA in developing and maintaining an architecture that is mission enabling, integrated and efficient. Subject to the issuance of service requests, the Contractor shall:

a. in conjunction with ITCD, engage stakeholders to proactively seek to understand their business challenges and needs before enabling architectural decisions;
b. act collaboratively to promote Agency-wide interaction in everything that it does;
c. foster transparency by making all of its decisions and artifacts available for Agency-wide consumption as is practical given security constraints and stakeholder concerns;
d. be agile so that it can respond quickly to changing business priorities, requirements, and demands from internal and external stakeholders;
e. communicate effectively to foster understanding about the role that enterprise architecture plays in enabling the stakeholder to meet its goals;
f. value diversity when as it seeks to facilitate building a consensus between NASA stakeholders in developing and gaining buy-in to future state architectures, implementation plans, projects, and operations;
g. build trust by ensuring all of its activities are aligned and in support of our stakeholders' needs;
h. promote innovation by providing visibility into how new technologies can be applied,
i. demonstrate competence in their broad understanding of the NASA business environment, and how the strategic use of IT can help enable business achievement,

j. capture and maintain the elements of the Current State Architecture used in determining gaps with the Future State Vision and obtains consensus with the Agency's stakeholders; and
k. develop the Future State Vision and maintain the Current State Architecture in the same general format to enable comparisons, gap analysis and trending data reporting.

The Current State Architecture does not attempt to document everything. Only the information that is necessary to make strategic decisions are documented and/or maintained. When persistent data is required, maintenance should be a matter of process and not a discrete activity.

The HQ Enterprise Architecture Team expects the Contractor to adhere to EA overarching principles. The Contractor shall:

a. integrate Enterprise Architecture throughout the business lifecycle and not as a discrete activity or independent activity;
b. provide enhanced understanding for decision makers to make informed decisions;
c. use Enterprise Architect as a strategic tool before decisions are made so that the decisions are founded in logic based on the Agency's vision, Strategic Plan, customer requirements and current assets; and
d. employ Enterprise Architecture as a distributed responsibility; many domains of expertise influence all areas of architecture development.

It is anticipated that NASA will have an EA program plan baselined by the start of the HITSS contract and each NASA center will have an EA plan consistent with the Agency direction. The HITSS Contractor shall:

a. adopt the HQ center EA plan and make recommendations for improvement within the first 240 days of contract award; and
b. maintain, update and assure alignment with the Agency EA plan and with the EA plans from other NASA centers to most appropriate level.

DRD	Description	Frequency
DRD #8	HQ Enterprise Architecture Plan Updates.	240 days after contract start date.

3.2 Operational Level Agreements

The Contractor shall develop Operational Level Agreements (OLAs) as necessary with other Contractors (e.g., I^3P Contractors and other HQ Contractors) to ensure clarity regarding availability, responsiveness, functionality and return to service. To provide transparency to NASA customers and providers, OLAs shall be in a consistent format, be published and available. Variance reporting is required as needed.

DRD	Description	Frequency
DRD #9	Operational Level Agreements.	In accordance with Government schedules.

3.2.1 Problem and Incident Management

The Contractor shall implement and sustain Problem and Incident Management Processes in accordance with the NASA OCIO ITIL implementation strategy. The contractor shall implement and sustain Problem and Incident Management Processes with the goal of preventing problems and resulting incidents from happening. The purpose of Problem Management is to provide a pre-defined and approved process for managing the lifecycle of all problems to include diagnosis, determination of resolutions, implementing solutions through appropriate control and change management procedures, trending and preventing problem recurrence. The purpose of Incident Management is to deal with all unplanned interruptions to an IT service or a reduction in the quality of IT service. This can include failures, questions or queries reported by users via telephone, email, face-to-face, or automatically detected and reported by event monitoring tools. The primary goal of Incident Management is to restore normal service operation as quickly as possible, minimize adverse impact on business operations, document sufficiently to facilitate substantive analytics (e.g. root cause), and ensure that the best possible levels of service quality and availability are maintained. The contractor shall implement and sustain a work management tracking system to ensure effective Problem and Incident Management. The contractor shall be responsible for:

a. designing and implementing Problem and Incident Management procedures;
b. identifying problems by proactively performing on-going trend analysis on Incident information;
c. documenting, tracking and managing all problems and incidents;
d. investigating and diagnosing problems in collaboration and coordination with Government, I^{3}P contractors and other contractors;
e. retaining ownership of each problem/incident assigned by either the Enterprise Service Desk or Government Service Integration Management (SIM) office;
f. validating problem workarounds;
g. maintaining regular communications between all parties to include ITCD, HQ users, the Enterprise Service Desk, the Service Integration Management office, and other NASA contractors as appropriate;
h. performing Root Cause Analysis and as appropriate develop Corrective Action Plans;
i. resolving problems/incidents in collaboration and coordination with ITCD and other NASA contractors such as I^{3}P contractors.

DRD	Description	Frequency
DRD #10	Report on response times, ticket aging, and customer satisfaction, delivered.	1 month after contract start date and monthly after that.
DRD #11	Root Cause Analysis and Corrective Action Plan.	As requested by ITCD.

The following metrics are associated with Problem Management during Prime Time hours:

Metric	Description	Performance Level to Achieve Fee
Metric #4	Problem Ticket Response Time. Respond to problem tickets within 4 business hours (time to first response), resolution time within 3 business days, and user completion notification within 4 hours of ticket closure.	Meet metrics 93%-96% of the time.
Metric #5	Prime Time Password Resets. Respond to application password reset requests during Prime Time hours within 30 minutes and accomplish resets within 60 minutes.	Meet metrics 90%-95% of the time.
Metric #6	Restore Prime Time Service Outages for Applications and Servers. For service outages affecting more than one person, respond within 5 minutes with daily updates provided until the outage is mitigated.	Meet response and mitigation metrics 90% - 95% of the time.
Metric #7	Resolve Prime Time Application and Server Hardware and Software Problems. For reported hardware and software problems, respond within 30 minutes with a fix accomplished within 12 prime-time business hours.	Meet response and mitigation metrics 90% - 95% of the time.

3.3 Configuration Management

Configuration management (CM) is critical to HQ’s complex integrated IT environment as it provides process and products that assure or aid in the clear and accurate understanding of our IT assets, their function (services provided, etc.), their form (platform, OS, etc.) and their fit (location, reliance, dependency, etc). Accurate CM is the cornerstone for efficient operations, effective IT Security, and agile adaptation to change. The contractor shall maintain and enhance the HQ’s CM program, incorporating all practical portions of the existing ITCD CM practices and adapting and modifying the program as new conditions and requirements arise.

A motivating driver for a quality CM program is to assure appropriate rigor is applied to project execution and that changes to the infrastructure do not adversely or unexpectedly impact services, costs, or inhibit strategic goals. It essential that the review processes (e.g. Service, Request Review Team. Service Requirements Review, Preliminary Design Review, Critical Design Review, Test Readiness Review and Operational Readiness Reviews) are adhered to and that documentation is accurate, current, and complete (e.g. Systems Description Document, Version Description Document, Change Requests Documents, Security Review Documents, Design Specification and Requirements Specification).

One of the CM goals is to communicate our baseline and our changes to a wider community. To meet this goal and to automate the process, NASA has implemented a search and query service that traverses essential infrastructure information sources (BIANCA - Business Impact Analysis for Networked Computer Assets), which provides access to ROSA, SOPR, Change Management, DNS and other sources that when aggregated gives a total view of the system or service. Because the utility of this service is reliant on the accuracy of the source data, the contactor shall ensure that the sources are maintained, kept up-to-date and ensure secured web access to baseline documentation, linkages to procedures, linkages to applications and the ability to view from system, service, customer, portfolio and other query vectors.

3.3.1 Configuration Management Plan

The Configuration Management Plan may require updates to adapt to new processes, organizational structures or technologies. The contractor shall maintain and enhance the existing IT Configuration Management Plan that describes how CM shall be maintained and how new capabilities will be implemented across the contract including ease of availability and search for baselined and version controlled documents, as-built drawings, change packages, Standard Operating Procedures, Policies, Interfaces, Agreements and other artifacts which collectively comprise the HQ IT Architecture.

DRD	Description	Frequency
DRD #12	Configuration Management Plan.	Update as required by ITCD.

3.3.2 Configuration Control Board Support

The Configuration Control Board (CCB) is an open meeting that invites participation from our customers and providers. In support of ITCD's administration of the CCB, the contractor shall support approximately 270 milestone reviews per year half of which are formally presented at CCB and half are reviewed "out of board" via email. Additionally, the contractor shall:

a. set up meeting rooms, maintain notification lists, provide supporting material and schedules, and provide CCB minutes posted within one (1) business day assuring completeness and accuracy of documentation;

b. ensuring integration of all HQ contractors and customers into the process;

c. compiling, coordinating, providing and in executing the agenda for the CCB;

d. management, coordination, execution and reporting of the review processes (e.g. PDR, CDR, TRR, ORR);

e. management, coordination, execution and reporting of the requirements processes to assure consistency, completeness and alignment; and

f. supporting new requirements to integrate change process and configuration control with the NASA Data Centers at JSC, the NASA Enterprise Applications Competency Center, the NASA Shared Services Center (NSSC), and potentially other NASA, Government, and commercial service centers.

DRD	Description	Frequency
DRD #13	CCB Meeting Minutes.	Weekly – 1 day after meeting.

3.3.3 NASA HQ Data Center Configuration Management

The contractor shall perform CM of all data center hardware and supporting infrastructure, operating system software, as well as standard operating procedures and documentation developed or maintained by and for the HQ Data Center. The contractor shall process and execute successfully approximately 200 change requests per year (approximately 12 change packages 'in-work" at any time). Specifically, the contractor shall:

a. keep this documentation up-to-date within 2 business days;

b. securely store and make continuously available to NASA management and the HQ IT Security team administrative passwords and similar credentials contained in the data center safe;

c. maintain and provide visibility to an inventory of systems, appliances and subsystems that are part of the Data Center and the Systems Engineering Facility and similar physical assets;

d. maintain and provide visibility to an inventory of spare parts sufficient for emergency repairs; and

e. maintain written detailed documents at the same levels that reflects the current configurations of servers, cable distribution, rack distribution, inventories, licenses, systems descriptions, and changes.

DRD	Description	Frequency
DRD #14	Spare Parts Inventory Report.	90 days after contract start date, quarterly thereafter.

3.3.4 Application Configuration Management and Version Control

To aid application sharing and code re-use and to mitigate risk of loss or loss of continuity to the government, the contractor shall use a NASA hosted code library as HQ's single authoritative source for the development, packaging and release of application software developed at HQ. The contractor shall assure that all application packages and versions are entered and maintained in the HQ Subversion (SVN) /Trac system (aka STACR) service and is available to all of their developers, designated NASA employees and that index and inventory data is available for query outside of the SVN system.

3.3.5 Catalog of Current Software Applications

The contractor shall use the NASA-provided Repository of Supported Applications (ROSA) system, and update, augment, validate, and maintain current the HQ's catalog of application assets (those in development, production, or archived locally). Specifically, the contractor shall:

a. document requirements, design, code, test scripts, planned test results, actual test results, number of customers, software version, version description documents, all current fields in the application documentation in the HQ documentation repository (ROSA) and queryable via BIANCA;

b. inventory all HQ applications regardless of host or network (e.g., mainframes, virtualized hosts, etc);

c. inventory all sites and web applications that are developed and maintained by the contractor;

d. ROSA will be kept current and documentation shall be posted within 24 hours as CCB milestones and related activities are completed;

e. report changes to ROSA via an automated method, provision a quarterly summary view; and

f. provide both machine-to-machine and human access.

DRD	Description	Frequency
DRD #15	Summary of updates to ROSA showing what was modified over previous 3 months.	Available quarterly.

3.3.6 Diagrams of Applications, Services, Servers and Networks

Diagrams of our services are an important asset for analysis, modeling, problem solving and conveying ideas. Graphic depictions will be used by NASA and contractor management staff in order to visualize the relationships between and the characteristics of the various production software applications, services and hardware and will be reused to generate analysis, code, and work-flows. Graphic representations need to be accurate and versioned. Each should retain sufficient annotation to enable linkages via BIANCA and other queries. They can be computer generated but must be available in formats that lend themselves to editing and reuse and not only in static (jpg) format. Generating these diagrams is an important part of our overall CM service. The contractor shall:

a. provide, update, augment, validate, and maintain current graphic depictions of logical and physical connectivity and relationship (e.g. communication paths) of servers, services and functions of all supported hardware and software within the NASA HQ facility or tied logically to HQ services (e.g. a network extending to another building);

b. graphically illustrate the various supported production applications, their interfaces among themselves, get versus pull, logic and services;

c. provide ability to link graphic representations together when browsing between logical and physical representations;

d. provide versions that are machine processable (e.g. UML);

e. be web viewable and editable regardless of OS;

f. indicate authorship, validation, revision and currency and adherence to proper names of applications and services for data consistency and to provide machine assisted linkages;

g. be linked to similar relevant supporting documentation; and

h. be discoverable by search or query of the similar systems, applications, hosts or services.

DRD	Description	Frequency
DRD #16	Diagrams of Application logic, connectivity, interdependence and data flow.	90 days after contract start date and update continuously.
DRD #17	Diagrams of Server dependencies (sinks/sources), physical placement and relationship.	90 days after contract start date and update continuously.

3.4 NASA IT Infrastructure Library (ITIL) Version 3 Approach

As the Agency Chief Information Officer's (OCIO's) vision is to use Version 3 of the ITIL framework as the NASA IT operational model, the Contractor shall be capable of implementing elements of this model at HQ. ITIL version 3.0 focuses on Service Management and seeks to align IT with business objectives. ITIL version 3.0 outlines a set of integrated processes that encompass the full scope of the IT service lifecycle. By defining a common set of ITIL version 3.0 aligned processes, HQ strives to attain maximum efficiencies while ensuring seamless, integrated services for IT customers. The contractor shall, at a minimum, support the ITIL-3 processes as they are implemented in accordance with the OCIO.

- Incident Management
- Problem Management
- Request Fulfillment
- Change Management
- Configuration Management

3.5 Safety

Safety for NASA's civil service and contracted employees is a top priority. The contractor shall implement and maintain a comprehensive safety, housekeeping, and health program for all assigned areas and activities. In this regard, the contractor shall:

a. develop, submit, implement, and maintain a Safety and Health Plan. The contractor shall submit reports on occupational injuries and illnesses experienced by contractor personnel in an Occupational Injuries and Illnesses Report;

b. comply with applicable NASA safety standards and reporting requirements, and ensure that the proper handling and/or disposition of hazardous materials and waste are observed;

c. conduct quarterly, and unscheduled, safety inspections of the NASA HQ Data Center, the User Resource Center (URC), and other areas in the HQ building or other HQ facilities that are administered by the contractor. The results shall be reported to the COTR and the HQ Safety & Occupational Health Manager as part of the Occupational Injuries and Illnesses Report; and

d. conduct periodic safety and health training for all contractor employees, and promptly report matters of concern to the COTR and CO. The contractor is encouraged to make recommendations and to actively participate in supporting NASA in improving the safety and health environment of HQ in addition to the contractor's facilities.

Data Center and Systems Engineering & Integration (SE&I) Lab facilities shall be neatly organized and kept clean at all times. The contractor shall:

a. report any safety issues related to the Data Center and coordinate all activities to resolve them; and

b. maintain strict and orderly computer rack and wire distribution, maintain continuously updated “as-built” diagrams and maps of the HQ Data Center and be responsible for a clean, clutter free, professional environment.

DRD	Description	Frequency
DRD #18	Health & Safety Plan.	Submit with Proposal; update if directed.
DRD #19	Occupational Injuries and Illnesses Report.	One month from contract start and monthly thereafter.

3.6 Records Management

The contractor shall maintain data qualifying as Federal records in compliance with Federal and Agency records requirements as required by the Federal Records Act, 44 U.S.C. §§ 3101 et seq. as codified in 36 CFR 1220-123 and including Federal Enterprise Architecture (FEA) Records Management Services functional requirements. NASA HQ owns the rights to all electronic information (electronic data, electronic information systems, electronic databases, etc.) and all supporting documentation created as part of this contract. In support of Records Management the contractor shall:

a. effectively and efficiently manage records, regardless of format or media (including paper, microform, electronic, and audiovisual);

b. preserve, maintain, and only dispose of NASA records in accordance with authorized retention schedules such as NPR 1441.1, NASA Records Retention Schedules and the National Archives and Records Administration’s General Records Schedules. Destruction of any Federal records, regardless of format, without an approved schedule is a violation of Federal law;

c. where the contractor develops or provides systems or applications, the contractor shall ensure that records management and records archival functions are addressed in the requirements phase for the design, development, and implementation of new or significantly revised information systems;

d. ensure systems protect the trustworthiness of electronic records, including their reliability, authenticity, integrity, and usability to meet its internal business and legal needs, as well as external regulations and requirements; and

e. for systems or applications created or supplied by the contractor that contain Federal records, sufficient technical documentation of the system or application such as design and maintenance records are Federal records and shall be managed as such.

4.0 Customer Relationship Management

A goal of this contract is to provide IT services that enable HQ employees to conduct their business effectively and efficiently. A key component of delivering successful services is establishing and maintaining good customer relationships. To plan, establish, and manage these relationships, the contractor will support the development and implementation of a customer relationship program. The program includes identification of key stakeholders and change agents, customer communication, customer business process knowledge, customer problem tracking and mitigation, customer training, and identifying and facilitating customer solutions. The contractor shall serve as an agent for ITCD and simultaneously serve as a customer advocate. The contractor shall work with customers under the direction of ITCD to identify problems, opportunities, requirements, and risks. In collaboration, ITCD and the contractor shall identify solutions and mitigation strategies to deliver effective IT solutions geared to customer's requirements. Contractor employees may at times be the first point-of-contact for HQ customers. In all instances of customer contact, contractor employees shall adhere to an approach that "One call does it all". Accordingly, when a customer makes an initial request to the contractor, the contractor shall ensure the request is routed to the appropriate service provider correctly (regardless of contract vehicle), communicated to and, if required, approved by ITCD Customer Service Managers. If the HITSS contractor is responsible for completing the action, the contractor shall make contact with the customer to provide periodic updates and ensure that the action was completed to the customer's satisfaction.

4.1 Customer Service Model

The contractor shall provide a consolidated approach to delivering a comprehensive range of end user support services for HQ employees.

Essential for building a strong relationship with customers is an effective Customer Service Model that focuses on understanding customer requirements and values and consistently monitors customer feedback for signs of problems or difficulties. The contractor shall implement a customer service model that:

a. is perceived by each individual customer as competent, responsive, and timely

b. supports all ITCD programs, projects, and services. Contract staff shall identify themselves as contractors representing all ITCD programs, regardless of where the end service is provided;

c. anticipates issues, concerns, and problems and preemptively initiates resolution;

d. encourages and facilitates customer self-sufficiency;

e. effectively develops and disseminates information regarding available services and technologies, system outages, new initiatives, etc.;

f. effectively coordinates with ITCD Customer Service Managers, HQ Organizational IT Points of Contact, Task Managers, the Enterprise Service Desk, and other contractor Customer Service representatives to provide a uniform approach to customer service;

g. understands the evolving IT requirements of the customer;

h. coordinates with ITCD to ensure recommendations and approaches can be supported;

i. coordinates with IT Security to ensure any recommended solution or changes are secure;

j. provides a method, subject to NASA approval, to obtain after-hours emergency support (defined as support for senior NASA officials, time-sensitive critical action, or a service interruption that involves a significant percentage of the HQ population);

k. proposes, for Government approval, metrics that describe service delivery activities to measure contract performance with regard to service delivery, customer feedback, quality assurance and timely delivery of products and services; and

l. provides contractor developed surveys and the means to administer them. Provides continuously available customer feedback and other information to the Government of sufficient detail to identify trends and gaps of customer requests for service and services rendered; and incorporates ITIL3 principles and practices to align with NASA service delivery and provide continuous service improvement.

DRD	Description	Frequency
DRD #20	Customer Service Metrics Proposal.	Deliver within one month of contract start.
DRD #21	Customer Satisfaction Survey Report.	Deliver at contract start with the customer satisfaction survey, monthly summary analytics and trending.

Metric	Description	Performance Level to Achieve Fee
Metric #8	Customer Satisfaction Surveys. Achieve a "4" or "5" (on a scale of 1-5 with 5 being the highest) on customer satisfaction surveys. (a minimum number of surveys received will be established).	Customer surveys shall include an Overall Rating of no less than a “4” (on a scale of 1-5 with 5 being the highest).

4.2 User Resource Center (URC)

The contractor shall operate and maintain an on-site User Resource Center that provides generalized and specialized IT information and support for small ad-hoc and walk-in requests, currently approximately 69 customers per month. The contractor shall keep abreast of current and emerging technologies that are relevant to the NASA IT environment and mission and serve as office environment experts for advice. The User Resource Center shall accommodate walk-in customers and be available from 7:30 AM to 5:00 PM, Monday through Friday excluding holidays. Services available in the URC include:

- Scanning
- File conversions
- Above core applications (e.g. Photoshop, Visio) assistance
- File archiving to CD

4.3 Customer Education and Outreach

The Contractor shall provide customer training, end-user documentation, and communication activities for IT applications, services, and issues that affect the HQ user community (NASA employees, contractors, and NASA HQ consultants). The contractor shall provide training using classes, video files, online content and printed materials. Classroom training will be conducted in the on-site training facility (Computer Training Center), Monday through Friday, except Federal holidays, between 8:00 a.m. until 4:30 p.m. local time.

ITCD's IT communications program provides strategic, tactical, and proactive communication support for HQ CIO and all supported IT projects/programs. The contractor shall provide customer communication support, including development, maintenance, and execution of the ITCD Communications Plan. Program support includes content development and maintenance of ITCD-managed Web pages; identification of stakeholders/audience; message delivery methodologies; message timing; message content; technology to business terminology translation. Additionally the contractor shall provide timely submission for recurring outreach messages, including NASA HQ Web sites, HQ Facebook page; Heads Up articles; and others as defined. Specific outreach will also be required to communicate "IT Notices" and associated distribution list. The contractor shall support the drafting of approximately 10 IT Notices per month.

The contractor shall provide training for IT applications and services. The contractor shall develop and document a Training Program approach and framework and provide to the government within two months of contract start. Training methods shall include one-on-one, group, instructor led, remote, tutorial self paced, virtually over the web, and on recorded media. Training is required for both legacy applications and newly development applications. In addition, HQ users are increasingly impacted by NASA applications and services housed outside of HQ, and HQ is at times called upon to develop and/or deliver end-user documentation, outreach and computer training if no existing materials are available prior to deployment at HQ. Training materials shall be provided for both instructors and students to facilitate use of applications and solutions provided or supported under this contract. The contractor will recommend the appropriate training scope for each project for government approval and should include approach, timing, dependencies, and audience. The contractor shall schedule and facilitate training sessions including facilities and equipment.

Customer advocacy and coordination groups will be supported and facilitated by the contractor. This includes recurring meetings for the Customer Service Project Reviews and Customer Advisory Committee. Coordination and communication with customer advocacy groups is a critical success component for ITCD projects.

The contractor shall support NASA in planning for and implementing change associated with new IT capabilities within HQ and the Agency. NASA may call upon the contractor to provide support not only for HQ-specific system implementations, but also for Agency-wide initiatives that may impact HQ's infrastructure, processes or policies. Those activities include impact assessment of proposed change(s), modification and coordination of required changes, and documentation of change management processes and procedures.

The contractor shall develop, submit and regularly update the Training Program and Outreach Plan detailing plans during the upcoming period and the top five to ten quantifiable objectives expected to be achieved. The Government and Contractor will discuss, modify (if necessary), and agree to the top five to ten objectives, which will form the basis for a portion of the incentive fee determination (technical performance) during that period. The contractor shall release an update to the Training Program and Outreach Plan every six months. The contractor shall submit a report at the end of each period to describe the accomplishments against the objectives met from the previous period and which 5-10 objectives will be targeted for the next period. The Training Program and Outreach Plan shall adhere to the guidance in section 2.3.1 and 2.3.2 of this Performance Work Statement.

DRD	Description	Frequency
DRD #22	Training Program and Outreach Plan, detailing materials, methods and approach and to include communications, and facilitating relationship building activity. Initial plan and updates shall be submitted on time.	One month from contract start.
DRD #23	Customer Advisory and Service Review, meeting notes, action items, results, and schedule.	As required within 2 business days of meetings.

4.4 Event Support

The contractor shall serve as the IT expert for events requiring audio-visual services at HQ and provide support to separate contractors whose responsibility centers on operating the HQ A/V equipment and facilities. IT support includes both on-site and off-site activities such as providing and configuring the necessary IT hardware and software, checking LAN connections, interfacing with other systems or facilities, providing dedicated support for the entire length of multi-day meetings, training the A/V contractor who operate the A/V equipment, and coordinating with multiple organizations and contractors. The contractor shall develop standard procedures available at contract start for obtaining advance coordination for A/V IT support. Work products and procedures must also adhere to standards of federal web publishing, IT security and Section 508 conformance along with all other applicable federal, Agency and departmental regulations.

4.4.1 Web-Streaming

The contractor shall operate and maintain the Headquarters Web Streaming services ensuring effective delivery of content provide by NASA TV. In support of NASA events which occur at on-site and off-site locations the contractor shall provide services to digitally capture events and meetings for the purpose of live Web-streaming, post event Web-streaming, or event recording. The contractor shall support approximately 4 Web-streaming events per month. The contractor shall:

a. ensure proper coordination with public affairs, NASATV, and others is maintained to ensure reliable and timely broadcast of content through the HQ streaming media servers;
b. ensure that the HQ streaming servers are maintained and are compliant with correct compression and service requirements of NASA TV and the Agency portal;
c. participate in the planning, coordination, and setup of video recording and streaming of NASA events with event planners and hosting locations;
d. provide on location technical staff to record NASA events using provided portable recording and encoding systems for posting to websites, DVD releases, or streaming over the web; and
e. evaluate new and emerging technologies to continually enhance service offerings associated with the capability to capture and Web-stream NASA events (live and recorded formats).

4.5 On-Boarding Support

The contractor shall provide support in the On-Boarding of approximately 34 employees per month (civil servant, contractor, temporary workers, remote users, etc.). The contractor shall support HQ in implementing process re-engineering as defined by the Agency On-Boarding Initiative for NASA (OBIN) project.

It is NASA's goal to equip all employees with the necessary assets to enable them to be productive on day one with NASA. This means that all IT assets such as computers, user accounts and system access is coordinated and delivered in advance of their start date. The contractor shall work with other NASA organizations and contractors to ensure this happens. These organizations include the following HQ and Agency offices: HQ Human Resources Management Division, HQ Security Office, HQ IT Points-of-Contact, HQ Administrative Officers, NASA Shared Services Center, and the NASA/ACES contractors. The contractor shall utilize the HQ Check In Check Out (CICO) system as well as the Identity and Access Management Tools (IdMAX). The contractor is required to take a proactive approach in On-Boarding and is sometimes called upon to support and help trouble shoot delays in on-boarding. The contractor shall participate in HQ and Agency level working groups aimed at continuous improvement in this area.

4.6 Service Coordination and Collaboration

Effective service coordination and collaboration with all internal and external customers is critical to the success of ITCD and the contractor. The contractor is required to coordinate services and collaborate with the following internal and external customers: HQ end users, ITCD, NASA leadership, I^3P Contractors, and other HQ and Agency contractors. The contractor shall support ITCD in the development of processes and procedures that will facilitate coordination and collaboration between contractors. ITCD must ensure that coordination and collaboration is effective and efficient. The contractor shall be prepared to report on issues or status regarding coordination and collaboration.

4.7 Service Management

A goal of this contract is to ensure proactive management of all requests for service from HQ customers. This includes Help Desk Management, Service Desk Management, and Service Request Management.

The contractor shall implement a service management program that provides comprehensive support in the planning for and execution of customer requirements. The contractor shall work closely with ITCD and become knowledgeable of individual Mission Directorates and Mission Support organization's mission, programs, and organizational structure, and work closely with their Points of Contact (POCs) and ITCD. The contractor shall support the Mission Directorates and Mission Support POCs in defining requirements for their organization; developing, tracking and coordinating schedules for their activities; and ensuring that configuration and inventory controls are maintained.

The contractor shall:

a. propose, for Government approval, metrics that describe service delivery activities to measure contract performance with regard to adherence to Customer Requirements which include; service delivery, customer feedback, quality assurance and timely delivery of products and services; and
b. anticipate issues, concerns, and problems and coordinate with ITCD to preemptively initiate resolution.

DRD	Description	Frequency
DRD #24	Customer Requirements Adherence Metrics Proposal.	Deliver within one month of contract start.
DRD #25	Requirements Adherence Report.	Deliver at contract start, monthly thereafter.

4.7.1 Help Desk Management

HQ intends for the HITSS contractor to use the NASA Enterprise Service Desk (ESD) located at and managed by the NASA Shared Services Center (NSSC) to manage all Tier 1 and 2 Help Desk calls. The ESD serves as the single point of contact for Enterprise Services (Tier 1) support providing a unified interface between the I^{3}P customers and the I^{3}P service providers (i.e. I^{3}P contracts – ACES, NICS, NEDC, EAST, and WEST). The Enterprise Service Desk ticket system utilizes the BMC/Remedy 7.5 software and sufficient license and access will be provisioned to the HITSS contractor.

For Tier 1 and 2 support the contractor shall work directly to resolve and triage calls directly and interface with the ESD for a number of activities. The contractor shall support approximately 520 HELP desk tickets per month. This includes (but is not limited to):

a. utilizing the same service as provisioned by the I^{3}P Tier 1 Enterprise Service Desk (ESD). The contractor shall leverage the processes and procedures to ensure close integration with ESD. The contractor is responsible for all integration work with the

NSSC. For reporting and analysis, the contractor shall leverage dashboard and analysis services functions provisioned by the ESD;

b. providing Tier 2 help desk support during the prime time work hours of 6 a.m. to 6 p.m. Eastern U.S. time on days when the federal government is open, even if contractually the contractor is closed on that day;
c. providing Tier 2 help-desk support via phone and e-mail;
d. reviewing all customer feedback received from the ESD customer satisfaction survey;
e. reviewing with NASA all surveys rated by customers as "dissatisfied" or "very dissatisfied";
f. providing 24/7 contact information and revising the information as necessary to keep it current;
g. providing and updating knowledge articles used by call agents to resolve and/or triage Incidents that pertain to HITSS specific contract service;
h. resolving, reporting status and closing escalated incidents that cannot be resolved at the Tier 2 level;
i. providing appropriate training materials in a compatible format and scripts to the ESD to help them triage calls properly;
j. providing and updating knowledge articles used by call agents to resolve and or triage Incidents that pertain to HITSS specific contract service. This includes knowledge articles for the Tier 0 self-service I^3P Web site for commonly identified incidents and or user self service activities;
k. providing notifications and community/organization lists for dissemination of planned and unplanned notices, service configuration changes affecting HQ customers for services provided by the HITSS Contractor;
l. providing status related to incident/problem resolution for those incidents assigned to the HITSS contract;
m. providing information to the ESD as to HQ specific configuration changes of importance for Tier 1 or Tier 0 levels;
n. providing escalation procedures to the ESD;
o. providing a POC for ESD-to-HITSS-Contractor escalation processing for both normal business and after hours;
p. providing metrics to the ESD as requested;
q. reporting all downtime, planned and unplanned to the ESD; and
r. providing initial load of Configuration Items (CIs) to the ESD/ESRS CMDB during the transition period of the Contractor or in accordance with a specific contract Service Asset and Configuration Management Plan.

Important ESD reference information can be found in the following documents:

- Enterprise Service Desk Concept of Operations
- Enterprise Service Desk Performance Work Statement and associated Appendices
- ESD/ESRS Interface Definitions Specification
- ESD/ESRS 7120.7 Program/Project Systems Requirements documents.

DRD	Description	Frequency
DRD #26	Summary and Trend Ticket Reporting including number of tickets opened, completed and pending (e.g. under a week, under two or over three) number escalated, rating, closed, times to first respond, customer satisfaction.	One month from contract start and monthly thereafter.

4.7.2 Service Request Management

The contractor shall efficiently receive and promptly process all Service Requests assigned to them. The Agency is migrating to the Agency-wide Enterprise Service Request System (ESRS). At contract start, however, HQ will not be fully utilizing ESRS. The Agency ESRS will be operational at contract start but will only be used for Service Requests assigned by the Agency to HQ for fulfillment. At some time in the future HQ will use the Agency ESRS for all HQ Service Requests. The current HITSS contractor is using the HQ ISEM Work Management System (IWMS). The contractor shall use the IWMS for performing Service Request Management. The contractor shall manage and support approximately 23 Service Requests per month.

4.7.2.1 HQ Service Request Management System

The current HQ work management system, IWMS, is a web-based collaborative tool that allows customers to create, track, and monitor the status of IT SRs. The contractor shall:

a. maintain web-based SR initiation and browse capability;

b. maintain user permissions based on specific tasks;

c. maintain standard permissions for any customer who does not have a system USERID;

d. maintain ability to initiate a new service request, search for existing service requests, run standard and custom reports;

e. maintain ability to browse the SR review agenda;

f. maintain ability to browse the CCB Agenda; and

g. maintain automatic notification via e-mail for any change in status of the SR throughout the SR lifecycle.

For all SR's submitted and within scope of this PWS, the contractor shall:

a. enter all SRs into the work management and tracking system within 12 prime time hours of receipt and shall enter the agreed upon SR completion date within three business days of SR receipt (approximately 25 SRs per month);

b. coordinate the CCB date or the completion date of all service requests with the customer;

c. complete service requests by the approved completion date, customer concurrence is required prior to Service Request closure;

d. coordinate any extension of completion dates with the customer. The COTR will approve requests for all extensions after two extensions have already been granted;

e. coordinate the closure of SRs with the customer. The contractor shall insure that SRs are closed within 72 hours of completion;

f. coordinate extensions to approved completion dates or project milestones with the customer and/or the HQ CCB. The customer and/HQ CCB has the right to disagree with the date proposed by the contractor. This shall be tracked as an unapproved completion date; and

g. provide a web-based customer survey appropriate to the work delivered. The first question shall be "Does the customer accept the work as complete". If the customer's answer is "no", then the work order shall remain open. If the answer is "yes" then the customer shall be provided with a customer satisfaction survey.

DRD	Description	Frequency
DRD #27	Service Request Processing Plan describing overall management and execution of the SR system and customer satisfaction report.	Within 2 weeks of contract start.

4.7.3 SR&QA Customer Surveys

Upon completion of each end user Service Request or Help Desk Ticket, the contractor shall conduct a web-based customer survey appropriate to the work delivered. The first question shall be "Does the customer accept the work as complete". If the customer's answer is "no", then the work order shall remain open. If the answer is "yes" then the customer shall be provided with a customer satisfaction survey. Contractor developed surveys and the means to administer them shall be demonstrated and delivered to the government for approval 15 days before contract start date. The contractor may use existing survey mechanisms such as the Enterprise Service Desk Remedy system.

DRD	Description	Frequency
DRD #28	Customer Satisfaction Summary and Trending Report.	One month after contract start, monthly thereafter.

4.7.4 Use of Agency Enterprise Service Request System (ESRS)

The ESRS is anticipated to be operational for Tier 1 requests during the phase-in of the HITSS contract in which case, the HITSS contractor shall receive service requests from the Agency Enterprise Service Request System for fulfillment. The HITSS contractor shall plan for a period of integration and testing to integrate their contractor order fulfillment systems with the ESRS.

As the Agency ESRS service matures, the HITSS contractor will continue to adopt the Agency service and migrate dependence from a HQ only solution. The specific interface definition between the ESRS and HITSS contract is defined in the ESD/ESRS Interface Definitions Specification.

The ESRS utilizes the same IT Service Management software as the Enterprise Service Desk ticket system (BMC/Remedy 7.5). The HITSS contractor shall interface with the ESRS for a number of activities. These include:

a. building interfaces between the ESRS Remedy system and the HITSS contractor system during the transition period. The contractor is responsible for all integration work with the NSSC;
b. building linkages between the NASA Enterprise Architecture Registry (NEAR) and the contractor system during the transition period;
c. fulfilling, reporting status and closing service requests and updating CIs (definition) in the ESD/ESRS CMDB (more definitions needed);
d. providing a POC for ESRS-to-HITSS-Contractor interfacing/integration for both normal business and after hours incident/problem resolution/service fulfillment; and
e. populating and updating HITSS service system and component information in the NASA Enterprise Service Catalog (ESC) in accordance with the NEAR IDS (NASA Enterprise Architecture Repository (NEAR): Interface Definition Specification).

4.8 Catalog Services

The contractor shall provide a full catalog of commercial IT components for ordering on the first business day of the contract. Each catalog entry shall clearly define, in precise and understandable terms, what hardware, software, service, coverage, warrantee, support, etc., is included in the catalog price. The catalog provided shall be on a commercial web-site with government pricing (e.g., pcmallgov.com; gtsi.com; cdwg.com, etc.) and shall meet all FAR requirements. The catalog provided shall allow alternate shipping methods. All NASA Headquarters employees may order from the catalog. The catalog provided shall also allow government employees to order items with their own personal credit cards and shipped to their residences. The contractor shall support between 500 to 800 orders per year. All items ordered for Government use shall be approved in the following sequence, first by the organization IT POC, then the organization budget official, and lastly the IT and Communications Division point of contract. The Contractor shall be responsible for delivery and when required, for installation of the product, except for desktop installations, which are performed by the ODIN vendor. For catalog items, the Contractor has no responsibility for integration into the customer's environment, consultation services, training, data conversion, or maintenance. If the product cannot be installed without causing anomalies with the customer's computer, then the product shall be removed and the customer's computer shall be restored to its original state. If problems occur after the installation that can reasonably be traced to the product, then the product shall be removed and the customer's system shall be restored to its original state. The catalog shall contain a disclaimer for each item that clearly limits the Contractor responsibility. The Government shall approve items and categories of items placed into the catalog.

DRD	Description	Frequency
DRD #29	Catalog Orders Report includes number of orders by category, number complete, funds used versus available, funds in process.	2 weeks from contract start, monthly thereafter.

5.0 Application Development & Information Management

Application Development provides comprehensive information services, delivering software and web applications to meet customer's business needs and search, query and information management tools to meet enterprise objectives. Much of the current HQ application inventory consists of legacy stove-piped applications that were replicated multiple times, so our challenge is to migrate as many of these instances as practical to a modern information framework that will extend reuse of data sources, information organization, and application functions while provisioning a faster more efficient environment to create and field applications.

This new environment will be guided by design goals of provisioning modern customer-facing interfaces, automated data exchanges from validated sources, and of reducing our dependence on specific hardware, and increasing our ability to employ analytics across our application inventory. Our objective is to provide decision support and knowledge services to the leadership of NASA and to support similar needs across the Agency.

The Applications Development program shall be aligned with Agency and HQ Enterprise Architecture, the ITCD Innovation Program, and Agency I^{3}P contract service providers. Success of the program requires clear communications with all stakeholders, establishing consistent and realistic expectations, delivering innovative, quality, timely, and cost effective solutions.

5.1 Establishment of an Application and Information Framework

Our goal is a comprehensive information service, efficiently delivering software applications and web sites to meet specific, though ever-evolving, customer business needs while employing a strategy that maximizes enterprise objectives. It is anticipated that business needs will be across multiple domains (e.g. finance, project management, facilities, capabilities, missions, legislative, organizational, etc) and that the formats of data sources will be equally diverse. As the content of applications (source, entity relationship, logic) often needs to be shared, leveraged, aligned or reused, the framework should provision methods for ingestion to search indexes, query services and registration as HQ-wide capabilities. Therefore a strategy beyond traditional warehousing will require a capability for data source management, link management, service relationship management, registration services, metadata management, data model management, data and service exchange management and linkages to monitoring and management controls for capacity planning, information usage and data and service exchange.

The establishment of a 21st century information management environment worthy of our customers and their mission requires the contractor to employ innovative thinking, complex problem solving, communication, customer relationship and organizational change management, strategic and tactical planning, adherence to documented process, technical expertise, and legacy support. The contractor shall deliver an Application Service Framework that is extensible and sustainable. The contractor shall:

a. develop plans to test and deploy the essential components of an application development framework;

b. ensure mechanisms for operations and management of services in the framework are integrated and supportable by the contractor as a critical element of each phased deployment;

c. restrict and otherwise minimize point-to-point service and data exchanges while promoting service advertisement, utilization, and management;

d. Data Exchange Agreements (DEA) will be migrated to fully automated service advertisements in order to maximize reuse of software functions and minimize point-to-point data exchanges;

e. automate DEAs sufficiently so that monitoring of success, schedule, and availability for more capacity can be determined;

f. ensure monitoring for every application and service that detailed records indicating customer use, including access, duration and relevant transactions are captured and viewable as a critical factor of determining performance and customer satisfaction;

g. ensure that vocabularies including data dictionaries, and metadata, and portfolio attributes are shared and used by a HQ search and query service;

h. adhere to goals of high availability and extreme responsiveness from a customer's point of view;

i. adhere to goals of hardware independence for customer environments regardless of OS and in support of mobile devices;

j. adhere to hosting goals of hardware independence, OS agnostics, and virtualized environments;

k. provision capabilities to add metadata elements of provenance and similar data validation and quality verification;

l. provision mechanisms to ingest data dictionaries, metadata, and similar sources in to search indexes and query builders; and

m. emphasize maximum flexibility in the use of customer facing interfaces that enable self service (e.g. query services, mashups).

The contractor shall develop, submit and regularly update the Application Service Roadmap and Implementation Plan detailing plans during the upcoming period and the top five to ten quantifiable objectives expected to be achieved. The Government and Contractor will discuss, modify (if necessary), and agree to the top five to ten objectives, which will form the basis for a portion of the incentive fee determination (technical performance) during that period. The contractor shall release an update to the Application Service Roadmap and Implementation Plan every six months. The contractor shall submit a report at the end of each period to describe the accomplishments against the objectives met from the previous period and which 5-10 objectives will be targeted for the next period. In addition to the general guidance in section 2.3.1 and 2.3.2 of this Performance Work Statement, The Application Service Roadmap and Implementation Plan shall address the following requirements:

a. an approach to improve/enhance the Software Management Guide and Application Development processes;
b. a description of the roles and responsibilities for developing, managing, and executing the roadmap and implementation plan;
c. a recommended software development methodology (RAD, Iterative, Agile, Spiral, etc.) and its integration to the SMG with emphasis on areas for modification and improvement to reduce cost and development time;
d. a recommendation for an Application Service Framework and a plan for implementing, testing and evaluating the essential components of the framework;
e. a communication plan that addresses the synergy and collaboration needed with other components of customer service, engineering/operations, security and all other applicable areas and addresses; monitoring of applications and related service, customer satisfaction of application services provided, and meeting performance and availability requirements;
f. an approach for analyzing the effectiveness/usefulness of existing tools and make recommendations for potential tool solutions that can support the Application Service Framework and related reporting;
g. a recommendation, plan and schedule for a Quality Assurance and Quality Control improvement process that addresses; number and type of applications, technologies in the application portfolio, the architecture of each application, type of data processed in the application portfolio; validation and verification of the application at critical milestones in the software development lifecycle;
h. an assessment of the existing test labs and test environment with recommendations for improvement;
i. an assessment of testing tools and reporting;
j. an approach for evaluating the existing information/knowledge management and CM tools;
k. a schedule for developing a plan for the evaluation of new and existing information/knowledge management and CM tools for recommended improvement, redesign, or replacement;
l. an approach for implementing and utilizing current investment in the IBM rational tools for areas of the framework;
m. an approach for reviewing and updating Application Development templates based on Application Framework recommendations;
n. a detailed description of the planning, requirements, design, development, verification & validation, and deployment disciplines that will be employed;
o. a description of how EA will be addressed in the plan and the verification points for ensuring that EA is part of the implementation plan;

p. a methodology for executing recommendations from analysis conducted on the SMG and App Dev processes;
q. a technical approach for how lessons learned and suggested improvements are recorded, tracked, and vetted; and
r. a managerial approach for monitoring execution of the plan.

DRD	Description	Frequency
DRD #30	Application Service Framework.	One month after contract start, modifications reflecting approved changes as required.
DRD #31	Application Service Roadmap and Implementation Plan.	Three months after contract start and every 6 months thereafter, modifications reflecting approved changes as required.

5.2 Support for Legacy Applications

NASA HQ has approximately one hundred applications of varying complexity and customer use. General business services supported by the existing application inventory include: Finance; Budget; Communication; Human Resources; Asset Management; Administration; and Program Management. Application types include several instances of Oracle and MS SQL databases with web interfaces via ColdFusion and reporting via Crystal Report, and simple Document Management services via Basis / Basis Webtop. The contractor shall be responsible for sustainment and maintenance of the current applications inventory while aggressively assessing which shall be consolidated, modernized, or decommissioned. Support for these applications will be provided until each has been dispositioned and our reliance on stovepiped infrastructure is reduced. The contractor shall evaluate each of the existing applications and provide a recommended disposition plan, including technology, data migration strategies, impact on operations, schedule and cost. The contractor shall conduct a quarterly assessment of the Legacy Application Portfolio with identification of the following:

- The number of legacy applications in the portfolio approaching end of life.
- The number of legacy applications in the portfolio requiring technology refreshes.
- The number of legacy applications in the portfolio with low utilization.
- The number of legacy applications in the portfolio with large footprints on the infrastructure and large resource consumption.
- The reduction of legacy applications in the portfolio.
- The reduction of maintenance required for applications.

The contractor shall develop, submit and regularly update a roadmap detailing plans during the upcoming period and the top five to ten quantifiable objectives expected to be achieved. The Government and Contractor will discuss, modify (if necessary), and agree to the top five to ten objectives, which will form the basis for a portion of the incentive fee determination (technical performance) during that period. The contractor shall submit a report at the end of each period to describe the accomplishments against the objectives. The contractor shall release an update to the Legacy Application Disposition Plan every six months. The contractor shall submit a report at the end of each period to describe the accomplishments against the objectives met from the previous period and which 5-10 objectives will be targeted for the next period. In addition to the general guidance in section 2.3.1 and 2.3.2 of this Performance Work Statement, The Legacy Application Disposition Plan shall define an approach for analyzing the legacy applications and a description of the roles and responsibilities for developing, managing, and executing the plan. The plan shall have a description of the methodologies for legacy application disposition that addresses the following:

a. analyzing and evaluating legacy applications for consolidation;

b. data migration strategies;

c. operations and management (O&M) impacts;

d. schedule and cost of implementing and executing;

e. records management considerations;

f. categorizing the types of legacy applications to support decision-making within budget, technology, data, and architecture as drivers for: Modernizing specific legacy applications within budget and determining appropriate enhancements for short-term use until a new application is developed to replace the legacy application; and

g. the identification of key factors for determining an application's end of life.

DRD	Description	Frequency
DRD #32	Legacy Application Disposition Plan.	6 months from contract start, modifications reflecting status and approved changes every 60 days.
DRD #33	Legacy Application Migration Report.	6 months from contract start, modifications reflecting status and approved changes every 60 days.

5.3 Support for Information and Knowledge Management

The existing HQ application inventory supports multiple business functions, ultimately influencing knowledge management and decision support, but often as a step-function outside the specific application. The contractor shall provide support for the development of information management and knowledge management capabilities to enhance NASA HQ in organizing and retrieving information, retaining and sharing knowledge, and furnishing information elements to support decision-making and minimize the steps required. The scope of this support includes modeling processes and workflows and providing improvements to NASA HQ offices in developing, maintaining, and implementing information and knowledge management architectures, ontologies, taxonomies, process models, and other tools and techniques that will assist NASA in meeting its knowledge management responsibilities.

The contractor shall provide technical support in assisting HQ offices in defining their information needs to support decision-making, in developing technical and business process solutions for obtaining and organizing the information, in protecting information that is sensitive and not appropriate for general distribution, and in defining and deploying mechanisms and tools for retrieving the information in an efficient, intuitive/contextual, and cost-effective manner.

5.4 Applications and Web Site Development

The contractor shall develop application software and web sites based on requirements and design specifications approved by NASA HQ (approximately 5 new (1.0) applications / web-applications per year and approximately 90 1.x releases per year). The contractor shall build software applications, establish baseline configurations, and perform such other tasks as are required to make the developed application ready for operational use. Formal configuration management controls shall be adhered to in coding application software and web sites. The contractor shall maintain the baselines under configuration management and enable current and continuous access to all application data and documentation. The contractor shall:

a. adhere to FIPS (Federal Information Processing Standards), Agency, and Division Standards;

b. adhere to the full range of application lifecycle management activities as defined in the HQ Software Management Guide;

c. formally propose modification to current standards prior to any deviation in accordance with the approved NASA HQ CCB;

d. document tools and technologies in the NASA HQ Application Technology Library;

e. prepare appropriate application and system documentation, (typically the software Version Description Document, an application Implementation Plan, and a User and Operations guide) prior to NASA acceptance;

f. adhere to interface controls including coordinating with computer operations and system engineering organizations within HQ and other NASA Installations to properly define operational and system requirements in the development of applications and in the planning of system capabilities. The contractor will document interfaces via Interface Control Documents and/or Memoranda of Understanding/Agreement and clearly depict times, flow, content and assure monitoring;

g. support hosting and development changes required to migrate relevant web and application services to I^{3}P providers;

h. develop data models to support design and reuse in accordance with target framework;

i. generate test data to ensure functionality and results prior to release;

j. deliver software test plans and test cases reflective of requirements and use cases;

k. deliver Logical Data Base Design and the Physical Data Base Design at the PDR and CDR. Data element and types, primary and secondary key fields, and dependencies among data shall be identified. Other pertinent characteristics shall be presented as determined by the contractor or directed by ITCD;

l. adhere to baseline requirements for all software documentation, including requirements, data sources, design, source code, test scripts, planned test results, actual test results, and version description documentation; and

m. maintain the baselines under configuration management and enable immediate and continuous access to all application data and documentation.

DRD	Description	Frequency
DRD #34	Framework for Development Program.	Due at contract start, modifications reflecting approved changes as required.
DRD #35	Interface Control Documents.	One month from contract start.

5.5 Software Management Guide (SMG)

The NASA HQ Software Management Guide gives specific guidance identifying the accepted life cycle processes that shall be used by the contractor for developing, prototyping, and deploying application services and is leveraged to extend or share our services outside of the HQ application development environment. The contractor shall:

a. utilize and enhance the NASA HQ Software Management Guide (SMG);

b. employ software management and development detailed in specific sections for Software Standards and Procedures, Software Configuration Management, and Software Assurance;

c. adhere to the NASA software policies and guidelines referenced, specifically NASA Procedural Requirements (NPR) 7150, NASA Software Engineering Requirements;

d. maintain and update to reflect current or needed processes and procedures, specifically to incorporate agility and responsiveness in development methodologies into NASA HQ standard; and

e. assure changes adhere to the CCB process and pre-submittal is reviewed by NASA for approval.

DRD	Description	Frequency
DRD #36	Software Management Guide.	Three months after contract start date, modifications reflecting approved modifications quarterly thereafter.

5.5.1 Streamlined Development Methodology

NASA HQ is striving to implement an iterative, streamlined Software Development Lifecycle as a means to deploy quality solutions quickly and to reduce design, development, and implementation risks. To transition/implement to a more rapid and iterative development methodology, the contractor shall:

a. use prototyping, and rapid development methodologies;

b. prototype new technical approaches, with an emphasis on small discreet proofs of concept;

c. demonstrate prototypes during critical design reviews;

d. ensure all derived requirements identified are presented to and accepted by the government prior to each design review;

e. provide full lifecycle documentation;

f. implement of an iterative development methodology in adherence to NASA 7120 and NASA HQ configuration management requirements; avoid using production data within a prototype application without prior government consent; and

g. modify the Software Management Guide.

5.6 Applications Development Requirements

Requirements are the foundation for the systems development program. A goal of this contract is to optimize the collection, documentation, and confirmation processes associated with the requirements phase of development. NASA HQ seeks to leverage technology for documenting requirements and facilitating mapping requirements to test cases and design specifications. In addition, improvements are sought in the means by which documented requirements are expressed back to the customer in an engaging way to verify and validate priority and intent. To facilitate requirements definition and to document independently testable and verifiable requirements, the contractor shall:

a. utilize existing NASA HQ defined tools (IBM Rational software) to document all software development project requirements, and/or recommend alternate technologies and approaches which provide improved efficiencies;

b. collect, interpret, model, generate, and document business, functional, and technical requirements in accordance with programmatic mandatory, preferred and optional formats;

c. provide a consultative role to fully elicit customer requirements,

d. ensure requirements traceability;

e. obtain written NASA approval of the documented application requirements

f. maintain responsibility to ensure captured requirements are vetted and understood by stakeholders prior to government acceptance;

g. ensure project requirements reflect the “as built” state of the product upon project delivery;

h. leverage technology, models, diagrams, and multimedia to communicate concepts and details;

i. provide business process re-engineering services as requested;

j. identify opportunities for business improvements and provide recommendations,

k. schedule and conduct requirements reviews to document and validate the NASA requirements;

l. consult with the Government data and/or system owner to support them in identifying the proper data category and security requirements in accordance with the governing FIPS (Federal Information Processing Standards) and National Institute of Standards and Technology Special Publications; and

m. ensure requirements reflect NASA HQ organizational approach to development projects and reflect the needs of the organizational unit and are not specific to an individual.

DRD	Description	Frequency
DRD #37	Standard requirements template that documents the service or design need from the perspective of effected discipline areas (e.g. applications development, IT security, customer training, operations) and by level of need (e.g. mandatory, optional, preferred).	Within two months from contract start date.

5.7 System Design Specification

Quality system design is the blue print that translates “what” the system must do to “how” the system will do it. A goal of this contract is to optimize the analysis, modeling, prototyping, documentation, and confirmation processes associated with the design phase of development. NASA HQ seeks to leverage technology for documenting design specifications and facilitating mapping design specifications to requirements and test cases. In addition, improvements are sought in the means by which design specifications are expressed back to the customer for confirmation. To facilitate system design the contractor shall:

a. identify and utilize a NASA HQ approved tool to document project design specifications,

b. map design specifications to requirements and test cases;

c. provide a repository for design specifications accessible using common metadata (e.g. portfolio, system, service, owner);

d. provide an Application Design Specification for each new development project and each subsequent project;

e. provide the system functional design, the software components definition, system interfaces, data base specifications, and systems, equipment and software requirements, as appropriate;

f. ensure design approach is vetted and understood by stakeholders prior to government acceptance;

g. ensure integration of modules or components through open reviews;

h. leverage technology, models, diagrams, and multimedia to communicate concepts, details, alternatives analysis, and technologies;

i. conform to the NASA HQ EA target architecture, including Master Data Management and web-service oriented architectures, NASA security and authentication standards;

j. give maximum consideration to both the short and long term requirements, including data consolidation, modularity, reusability, high availability, security, data access, data quality, and virtualization; conduct an alternatives analysis and recommend use of COTS, open source, cloud technologies as appropriate, and use of prototyping; and

k. provide and use modeling/analysis techniques to identify and correct design errors and deficiencies which could cause performance deficiencies or resource utilization and/or contention problems.

DRD	Description	Frequency
DRD #38	System Design Specification.	Two months from contract start date, modifications reflecting approved modifications as needed thereafter.

5.8 Data Conversion

The contractor shall provide data conversion support for moving and migrating data from legacy applications to formats required by modernization, consolidation or migration. The conversion efforts require creative and efficient approaches for applying various rule sets for the conversion processes, and for validating and verifying data accuracy. The contractor is responsible for successful project data conversion and data migration defects will be corrected at no cost to the government. The contractor shall:

a. work with ITCD, business customers, and system owners of the source and target applications so that they may fully understand the definition and characteristics of the source data and the converted data;
b. document data conversion rules;
c. provide consultation for improved efficiency and effectiveness in conversion and testing of the data;
d. provide NASA customers data reconciliation solutions; and
e. establish and operate of an information management authority to reconcile and harmonize NASA HQ data.

5.9 Quality Assurance & Performance Controls

NASA HQ seeks to implement repeatable application and information development processes that minimize errors, leverages previously employed solutions and maximizes service delivery to the customer. Additionally, all defects noted by the government during acceptance testing are deemed application defects for the purposes of this contract and will be remedied at no cost to the government. Defects will be defined as:

- Baseline Defects: the number of defects documented at the time of transition.
- Release Defects: defects identified after deployment that are introduced as the result of new or modified code, back end changes, or modification in application configuration. (ITCD reserves the right to update this definition based on the application portfolio. As the types of applications and their architectures change, review of the Release Defect definition will be required.).

To ensure project deliverables meet NASA HQ quality standards, the contractor shall:

a. establish and enhance quality assurance and quality control processes;
b. incorporate and identify a QA approach in each project plan;
c. establish, update and adhere to a method and process for code and system peer review;
d. develop and deliver a test plan for each project, regardless of project size or complexity including a pre and post deployment acceptance period;
e. validate requirements and design specifications;
f. complete all testing prior to government acceptance testing;
g. ensure products for acceptance testing includes a formalized assurance report as part of the documentation from contractor that confirms all requirements and design specifications have been met and the project is ready to be deployed in production, report should include test results and findings;

h. utilize QA practices to ensure defined procedures are followed and corrective action taken when procedures need to be modified;
i. document and communicate risks and issues identified in the QA program to NASA; and
j. be responsible for delivering a quality product as measured by the customer.

Application performance is measured at the user interface level based on customer impact. The contractor shall:

a. recommend performance metrics; provide tools and perform systems, performance, tuning, and capacity analysis studies for applications;
b. use modeling and/or prototyping techniques to quantify sizing of required resources;
c. identify and recommend system optimize opportunities and strategies; and
d. include performance planning approach in application design documentation.

5.10 Application Status Reviews

To facilitate NASA HQ's management of the Development Program, the contractor shall provide a monthly summary of development activities, including newly identified risks, recommended mitigations, and project status for cost, schedule, and quality. While the contractor may propose the format and full content of the Application Review Package, the package contents are to be coordinated with the government lead for application development, made available via the web and have a strategic focus. At a minimum the Application Review shall contain: schedules for applications currently in work; current project life cycle phase and project progress at the task level; project and program risks, issues, and both executed and planned mitigations; upcoming milestones; deployments planned for the current month; All current and anticipated schedule re-baseline requests; and the program project plan for the next two months, based on the Integrated Master Schedule.

DRD	Description	Frequency
DRD #39	Application Status Review materials.	One month from contract start date, monthly thereafter.

5.11 Application Portfolio Management

NASA HQ maintains a catalog of software applications, currently in our Repository of Supported Applications (ROSA). The contractor shall update, augment, validate, and maintain current the Catalog of Contractor Supported Applications to support in application sharing, re-use, portfolio management, migration and similar support activities. The contractor will be responsible for maintaining this information, current with each software and web site release. There are approximately100 ITCD supported applications and web sites managed through ROSA. Application data includes customers, service types, dependencies, system integration methods, and technologies and must align with or adopt agency nomenclature for portfolio categorization.

This catalog serves as a single document reference point for NASA and contractor management and staff for supported and active production applications. The contractor shall:

e. use existing tools when possible to perform the catalog function;
f. ensure the catalog includes applications that reside on all classes of computer platforms and networks, as well as all physical locations;
g. ensure the catalog includes all web sites that are developed and/or maintained by the contractor;
h. align where feasible to agency application portfolio categories; and
i. provide web-enabled access for ITCD and designated customers to the catalog.

The contractor shall analyze the current NASA HQ application inventory and submit recommendations throughout the course of this contract regarding opportunities to improve portfolio management, improve technologies, reduce operations and/or costs, improve data quality and availability. Project reporting will include identification of variances in portfolio strategies, impacts and risks. Additionally, the contractor shall include mechanisms to find, sort and analyze our portfolio by:

a. the number of legacy applications in the portfolio approaching end of life;
b. the number of legacy applications in the portfolio requiring technology refreshes;
c. the number of legacy applications in the portfolio with low utilization;
d. the number of legacy applications in the portfolio with large footprints on the infrastructure and large resource consumption; and
e. the reduction or trending of maintenance required for applications.

DRD	Description	Frequency
DRD #40	Portfolio Management Views of Application Services and Inventories.	Six months from contract start date, and maintained continuously thereafter.

5.12 Contractor's Development Environment

The contractor shall provide a managed and controlled environment in which it will conduct application development and testing. This environment shall include the appropriate hardware and software environment for the management of requirements, design, configuration management, testing and curation of the code base and interfaces. The development environment must be secure and be certified and accredited at no cost to the government. The contractor is responsible and liable for all security risk associated with this environment, including housing, storing, and transferring data. The government will be provided access to the development environment during normal business hours.

A goal of this contract is to leverage source code developed with public funding, open source, unlimited license and similar code release strategies to reduce costs and enhance the NASA HQ application portfolio. NASA owns all source code developed under this contract for use by NASA. The contractor grants NASA the right to use all source code provided by the contractor, but developed elsewhere, beyond the end of this contract. To ensure the quality of application development projects the contractor shall:

a. develop an explicit plan for project verification and validation that reflects current industry best practices and takes a life cycle approach to quality management;

b. provide development test plan framework within one month of contract award;

c. generate and use test plans, procedures, specifications, and reports;

d. provide test scripts and test procedures that are repeatable and under configuration control;

e. provide and utilize automated test tools for unit, integration, regression, system, and load testing identified in the test plan and utilized accordingly;

f. document test results, deviations from test procedures, and all software anomalies following completion of the testing;

g. prepare and conduct an acceptance test that demonstrates to the NASA customer the integrity of the application and prove that the application meets specified requirements; and

h. provide final and deployable application for the start of acceptance testing.

The contractor shall ensure that applications do not use production data for testing or otherwise prior to operational deployment, unless specifically approved by NASA.

DRD	Description	Frequency
DRD #41	As built detailed functional and physical description of development environment, its interfaces and processes.	Two months from contract start date, provided within 2 days of changes to structural or ITS environment including patches.

5.13 Application Deployment

The contractor shall deploy applications in the customer's computing environment following a successful Operational Readiness Review and pertinent training as defined in the SMG. For projects deployed to hosting facilities managed outside of this contract, the contractor shall meet all required steps for transitioning the project to the hosted facility for deployment. The contractor is responsible for identifying and following steps associated with deploying to hosting facilities, regardless the facility. The contractor shall:

a. deliver the User and Operations Guide;

b. baseline the final application documentation and source code;

c. maintain the baseline under configuration management control;

d. provide an Application Implementation Plan and Version Description Document for each software application and release that describes how the software is to be installed, tested and accepted by the user;

e. perform coordination with the data center hosting provider to ensure post-deployment success; and

f. perform coordination with the desktop provider (ACES) as required.

DRD	Description	Frequency
DRD #42	Application & Website delivery implementation plan.	Two months from contract start date.
DRD #43	Version Description Document.	Scheduled in accordance with CCB.

Metric	Description	Performance Level to Achieve Fee
Metric #9	Error Free Releases. All application version releases shall be error free and not require post-release repairs.	57% - 92% are error free.

5.13.1 Application Service Management Support and Administration

The contractor shall provide application and information management support for new and/or enhanced applications throughout the application life cycle. The contractor shall:

a. provide programming support for all applications of the DBMS;

b. collect and analyze selected DBMS data (at times from disparate data bases and application platforms);

c. support trade-off studies regarding selection of COTS, GOTS, MOTS, and open source DBMS products;

d. perform data administration and data base administration in accordance with operations guidelines;

e. coordinate with IT Security (ITS), Systems Engineering and Integration (SE&I), System Operations, I^3P contractors and all other organizational entities in identifying, fielding, debugging, and restoring services,

f. perform design and implementation of new data file structures and relations to meet requirements for data base expansion; and

g. perform data administration and data base administration activities to support applications, web sites, development activities, and post-deployment issues.

DRD	Description	Frequency
DRD #44	Application & Website delivery.	Two months from contract start date, available continuously thereafter.

5.14 Electronic and Information Technology (EIT) Accessibility, Rehabilitation Act of 1973

The contractor shall comply with Section 508 of the Rehabilitation Act (29 U.S.C. 794.d) as amended by the Workforce Investment Act of 1998 (P.L. 105-220). Section 508 was enacted to eliminate barriers in information technology, open new opportunities for people with disabilities, and encourage development of technologies that will help achieve these goals.

The contractor shall ensure, unless an undue burden would be imposed on NASA, that systems they develop, procure, maintain, or utilize electronic and information technology be accessible to:

- individuals with disabilities, who are NASA employees, have access to and use of information and data that is comparable to the access to and use of the information and data by NASA employees who are not individuals with disabilities; and
- individuals with disabilities, who are members of the public seeking information or services from NASA, have access to and use of information and data that is comparable to the access to and use of the information and data by such members of the public who are not individuals with disabilities.

The contractor shall comply with Section 508 technical standards for all EIT they develop, procure, and maintain. This includes the following technologies:

- software applications and operating systems;
- web-based information or applications;
- telecommunication products;
- video and multimedia products,
- self contained, closed products (e.g., information kiosks); and
- desktop and portable computers.

5.15 Support for HQ & Agency Forms

The contractor shall develop, implement, and maintain both Agency and HQ operational forms. "Forms" refers to paper forms and forms produced by electronic means. In support of this activity, the contractor shall:

a. design, produce, publish, and maintain Agency and HQ forms in both electronic media and hard copy; and

b. maintain a library (electronic and hard copy) of Agency and HQ forms via web access from the HQ home page and with electronic file transfer capability to NASA HQ organizations and field installations. The forms library has approximately 340 Agency forms and 245 HQ forms.

c. Create new or update forms. Approximately 48 form revisions are made each year.

6.0 NASA HQ Data Center

Data Center support at NASA HQ is divided between two major areas of responsibilities: the network infrastructure and the application and file servers that reside on it. The NASA NICS contract will manage and be responsible for all of the HQ's network infrastructure and support inclusive of firewall management, network address management, and the monitoring and management of routers, switches, cables and probes. The HITSS contract will be responsible for server management monitoring, maintenance and administration, inclusive of server and application deployment, troubleshooting and mitigation. The NICS and HITSS contractor teams must be well integrated and mutually supportive to assure that performance, availability and security are maintained at the highest levels practical and that moves, adds, changes, monitoring for performance, availability, capacity planning, reporting, and recovery processes are performed without organizational impedance.

The goals of ITCD are to provide uninterrupted service of our housed and hosted assets; to facilitate service advertisement and analytics; to provision continuity with similar data centers and alternative sites; to reduce the data center's impact on our environment; to reduce its size and; to eventually reduce our dependence on a HQ data center by reducing its size to the greatest extent that is practical. As such the contractor shall plan upgrades, process changes, monitoring tools, infrastructure modifications, deployment and audit methods in the context of an overall plan to migrate the HQ data center to it's optimum configuration within the Office of Management & Budget, the Office of the CIO and ITCD's guidelines and HQ building modernization schedule.

6.1 Data Center Operations, Scope

HITTS is responsible for the availability, reliability, and uninterrupted service of all servers, appliances, backup devices, storage devices, web streaming devices, data storage systems, server monitoring, and other similar systems and subsystems that reside within the HQ computer room and collectively provide customers with IT services such as databases, file storage and sharing, application and web hosting, authentication, and directories. The contractor shall:

a. coordinate issues of performance and availability of HQ resident services that are reliant on responsive network connectivity with the NICS provider;

b. provision machine processable Service Level Agreements which can be audited by all members of the agreement including the Government; and

c. properly label servers, cables and network devices and provide a means to easily locate server racks, network devices and telecommunication closets.

In addition to the IT services managed and hosted at the HQ Data Center, Operations also shares responsibility for services housed at HQ's but managed by external contracts (WEST/EAST/NDC, etc). To support their coordination role the contractor shall:

a. actively participate in configuration control, problem escalation/resolution, installation, and ITS with counterparts on other contracts or at other Centers in order to assure that failures of services are minimized; and

b. keep accurate, auditable as-build diagrams, POC documentation, OLA and Data Exchange Agreements (DEA), call-down return to service information, and ITS status for all items in the HQ Data Center.

DRD	Description	Frequency
DRD #45	Data Exchange Agreement diagram, performance and exception report.	One month from contract start date, and monthly thereafter.
DRD #46	Service Level Agreement performance and exception report.	One month from contract start date, and monthly thereafter.

6.2 Hours of Operations

The contractor shall provide on-site operations and maintenance support to all HQ systems. Support includes, but is not limited to, HQ based services, specialized services for commissions and study groups, file storage and data recovery, financial system portals, and similar services that are critical to business support for HQ customers. On-site support shall be provided during the Prime Time hours of 6:00 am until 6:00 pm Monday through Friday (except for holidays). During Non-Prime Time hours the contractor shall respond to the automated alerts, the Help Desk, or Government notification within 15 minutes. If the problem cannot be resolved remotely, arrive on-site within two hours of the initial notification.

6.3 Server Management Team (SMT) Operations

NASA HQ hosts general service as well as specialized application and file servers that, along with large storage, backup and other associated hardware, comprise the HQ service infrastructure. HQ hosted services include, but are not limited to, personal and organizational file storage, desktop backup servers and storage, database and web applications servers, RSA SecurID servers, LDAP and certificate servers, monitoring and intrusion detection servers, and streaming media encoders. These services are reliant on devices that include UNIX computers, mirrored Network Attached Storage devices, Storage Area Network devices, enterprise tape library system, Windows, Solaris and Linux Operating Systems, appliances, power supplies and monitoring equipment. HQ also houses agency services such as Internet Protocol Address Management (IPAM), Domain Name Service (DNS), NASA Consolidated Active Directory (NCAD), and intrusion detection devices. The service infrastructure largely conforms to a design goal of uninterrupted service. As a result, many of the servers are in a High Availability (HA) implementation and all are expected to be monitored 24 X 7. The goal for all of HQ hosted servers and appliances is to provide optimum performance and consistent availability to customers 99.99% of the time, 24 hours a day. The goal for HQ housed servers is the same as for hosted unless superseded by an ITCD signed or concurred MOU or OLA.

DRD	Description	Frequency
DRD #47	Availability of hosted and housed services.	One month from contract start date, monthly thereafter.
DRD #48	Performance of hosted and housed services.	One month from contract start date, monthly thereafter.

Metric	Description	Performance Level to Achieve Fee
Metric #10	Data Center Availability. Data Center systems and services (hosted and housed) shall be available on a 24 X 7 X 365 basis.	99.90% - 99.98% average availability.

6.4 HQ Hosted Server Operations

Hosted servers largely have services that are provisioned by HQ. For hosted services, the contractor shall:

a. maintain transaction and service logs of servers and services within the HQ computer center;

b. assure that quality and timely services are available;

c. assure performance is responsive to OLA and Government direction;

d. coordinate and perform upgrades;

e. maintain hardware & software;

f. enable accounts;

g. be actively engaged in problem coordination, analysis and resolution;

h. co-develop fail-over strategies, service integration, and budget planning;

i. administer, plan, manage and provision storage;

j. provide quantitative capacity planning;

k. provide security reporting, monitoring and management reporting, and Help Desk coordination; and

l. support in special projects to support Agency and HQ initiatives as well as special commissions and review boards.

6.5 HQ Housed Server Operations

There are several agency IT assets which currently provide critical services to the HQ customer community and to the successful operations of the HQ Data Center. Those services are housed within the HQ Data Center. and their configuration, management and monitoring is performed by Office of the Chief Information Officer (OCIO) organizational entities via the I^3P or other contracts. These include Active Directory servers/services, Internet Protocol Address Management (IPAM), (DNS/DHCP) servers/services and NCAD servers/services. Coordination for environmental issues, alert notification, trouble shooting, restoration and process modifications are some of the activities required by the HITTS contractor. To meet these responsibilities the contractor shall:

a. maintain and test a verified call list and escalation process;

b. coordinate and perform any needed environmental changes;

c. coordinate and execute needed configuration or restoration in conformance with CCB process;

d. co-develop process changes; and

e. report anomalous conditions.

6.6 Monitoring, Management and Capacity Planning

To facilitate lifecycle management, virtualization, migration, debugging and sound business processes the contractor shall provision a continuous monitoring capability that enables ad-hoc views and analytics of the HQ service infrastructure. Severs and services within the HQ Data Center are monitored using a robust implementation of Nagios that provides visibility in CPU, cache, I/O and other critical indicators that help determine use, availability, capacity and trends. The contractor shall support NASA in planning for and implementing changes to servers associated with determining the capacity and utilization of application servers and infrastructure servers. The contractor shall:

a. manage, install and maintain the performance monitoring and capacity planning tools at the HQ Data Center;

b. monitor for software performance and capacity planning changes inclusive of CPU utilization, memory usage and notify the performance monitor accordingly;

c. tune, adjust and modify systems and associated software for optimum performance within established security and CCB processes;

d. assess, with appropriate recommendations, the adequacy and effectiveness of solutions to hardware and/or software problems that are degrading computer system performance;

e. monitor and manage server use utilization including when it requires the insertion of equipment or agents into discrete components, devices, or the operating systems in order to identify and isolate anomalous conditions;

f. study trends, harvest and analyze data from existing management tool databases, develop new processes and procedures, and recommend innovations to ensure peak performance and availability of the service;

g. monitor, manage and provide trending views of services with data exchange agreements to assess the frequency and success of exchanges between those services within the HQ Data Center;

h. use structured and sound analytics to determine level of server use, peak use, and trends fact-based forecasts and modeling to assure levels of storage, memory, cache, and similar server subsystems are able to efficiently manage current services as well as determine capacity for growth or additional hosting requirements;

i. provide on-call, continuous support and shall respond within 15 minutes to the automated notifications from the HQ Data Center. Arrive on-site, if necessary, within two hours of the initial notification;

j. ensure agreements that document, manage, audit, and modify Data Exchange Agreements are in place between and across all relevant systems within the HQ domain. The agreements will be living documents used to assess performance delivery and reused to extend service;

k. operate and maintain all of the servers, data storage devices systems and subsystems that together comprise the HQ Service Infrastructure which provides services at HQ from inside the HQ campus or externally;

l. deploy and maintain all servers in accordance with the operating system and application configuration benchmarks published by the Center for Internet Security (CIS) as adopted by NASA Headquarters;

m. develop, acquire, secure, sustain, operate, or recommend system service enhancements, upgrades, or new capabilities. Proposed implementations shall provide an integrated approach with respect to existing systems, other work in progress, and applicable policies, standards, and methodologies while maintaining optimum security and performance;

n. coordinate hosting, relocation, enhancement and debugging activities with application development personnel, system administrators, the IT Security team, SE&I, Outreach, CM, and Help Desk, I^{3}P contracts, and any other group or individual that may be impacted by a change or require SMT to support a change;

o. support the service capabilities at service levels in accordance with OLAs that ensure that the availability requirements are satisfied. This support shall quickly respond to changes in technology, IT Security threats and incidents, dynamic requirements and system, equipment, software, service, and carrier outages;

p. notify ITCD as early as possible of the need for outages or reduced services due to IT Security threats and/or incidents, investigation of anomalous behaviors, equipment failure, or other contingencies that cannot be scheduled;

q. provide planning, definition, design, security, development, acquisition, implementation, maintenance and sustaining engineering support for new server systems or subsystems,

r. ensure that all CM documentation including diagrams, System Description Documents (SDDs), processes and procedures for the HQ Data Center devices and services is maintained and accurate;

s. develop, implement and maintain procedures, policies and standards to provide effective performance tuning and capacity planning such as service, memory, and processor utilization, and application performance;

t. provide analysis and growth projections for all supported systems;

u. provide and have accepted monthly capacity reporting and recommendations within 3 days of the end-of-month;

v. analyze performance of all supported systems (e.g. servers, storage systems, etc.) and provide monthly reports and have them accepted within 3 days of end-of-month. Performance Tuning will be accomplished to improve system performance; and

w. leverage data acquired and analytics performed to properly plan the data center's migration to its optimum configuration.

DRD	Description	Frequency
DRD #49	Diagram of server location.	Three months from contract start date, on-demand thereafter.
DRD #50	Diagram of servers logical connection to network.	Three months from contract start date, on-demand thereafter.
DRD #51	Capacity and Performance Report.	Two months from contract start date, on-demand thereafter.

6.7 Server Backups

The contractor shall perform regularly scheduled backups of servers and data storage devices in accordance with current SOPs. The contractor shall:

a. restore files on an on-demand basis;

b. conduct regularly scheduled quality assurance and process tests for the restoration process;

c. test the restoration process end-to-end at least twice each year and make recommendations. The first test shall be within the first 90 days of contract start

d. in the event of any contingency operations, current files and services must be available for recovery at remote sites; and

e. support the planning integration, coordination, and operations required to mirror selected files and storage devices at a designated remote location.

6.8 System Software Installations, Maintenance and Management

The contractor is responsible for assuring that server operating systems and affiliated libraries, patches and administrative software is up-to-date. The contractor shall:

a. monitor and report on system performance, availability and security;

b. participate or lead debugging and trouble shooting;

c. implement and maintain updates, corrections and enhancements to subscription services, operating systems and other commercial software packages;

d. ensure that licensing and certificates on servers do not expire;

e. ensure that all commercially released OS upgrades, software enhancements and patches are installed quarterly for Unix based servers (approximately 201 for Unix and 63 for Linux per quarter), monthly for windows based servers (approximately 250 per month) and on-demand for appliances. Security patches may occur out of normal scheduled upgrades. The contractor shall submit the appropriate Service Request to start the work so that the enhancement or patch can be completed on all supported devices within the year time frame requirement. The CCB process shall be used to govern the schedule should delays be necessary to:

f. ensure HQ Data Center software is in operating condition, current, with up-to-date maintenance, and is secure;

g. install and/or make updates to system software at a time that will not affect user productivity;

h. develop and maintain required test procedures or simulations to properly test software upgrades, modifications and maintenance;

i. provide an ongoing program to evaluate new commercially available software and provide reports including recommendations to designated NASA management;

j. ensure all operational support software modifications are installed, secure, work as expected and that no problems have been detected;

k. prepare a system software implementation test and release plan for each release or software package update and present it for approval of the performance monitor

l. maintain subscriptions to the OEM system software services;

m. review OEM web sites for failure, security, and enhancement information and install updates or patches as appropriate; and

n. manage and maintain hardware and software maintenance agreements for all production systems.

DRD	Description	Frequency
DRD #52	Quarterly/Monthly Patch Release Report.	One month after contract start date, monthly thereafter.

Metric	Description	Performance Level to Achieve Fee
Metric #11	Compliance with Patch Management Plan. Data center servers shall be patched in accordance with the approved patch management plan and schedule.	95% - 98% meet the criteria.

6.9 Equipment Upgrade Support

The contractor shall provide, at a minimum, a semiannual evaluation of new commercially available equipment for use in the HQ Data Center and provide recommendations to NASA management.

DRD	Description	Frequency
DRD #53	Equipment Upgrade Evaluation Report.	90 days of contract start date and semiannually thereafter.

6.10 Account Administration

NASA has implemented the NASA Account Management System (NAMS), as part of NEACC (NASA Enterprise Applications Competency Center. Currently, NASA HQ new application account requests, changes and deletions are processed through NAMS. HQ Account Administration staff receives notification from NAMS when all the required approvals have been made for account requests and proceeds with provisioning the application access. There are other, local, IT services where account provisioning and coordination is the responsibility of the HITTS contractor. This includes accounts for HQ network domain and data servers, Entrust Public Key Infrastructure (PKI), File Transfer Protocol (FTP), dial-in and HQ custom applications. In addition to using NAMS to provision access, the contractor will also use the HQ Check In Check Out (CICO) system for work orders involving access to user, shared and group folders. Among the responsibilities for account management, the contractor shall:

a. maintain up-to-date procedures for coordinating with IT Security, Help Desk, NAMS and others for account creation, modification and deletion;

b. provision password resets for local applications via the Help Desk processes;

c. provision user accounts for custom applications (approximately 50 new accounts and 50 deletions per month);

d. provision Entrust accounts (approximately 17 new accounts, 26 modifications, 17 disables and 4 PKCS12 public certificates per month);

e. provision the dbms for RSA tokens and notify customers for renewals (approximately 38 new tokens distributed per month);

f. create Guest Network accounts;

g. provision user requests for access to specialized Microsoft networked folders (approximately 30 per month);

h. provision new standard personal Microsoft networked folders;

i. support modifications to process and provide support to meet future NASA account services; and

j. adhere and comply with applicable regulations and policies (e.g., HSPD-12, NPR 2810.n, NASA PKI Registration Authority (RA).

The contractor shall support NASA Entrust PKI at HQ by providing Entrust PKI RA Administrators. Under the direction of the HQ PKI RA, the contractor PKI RA shall:

a. pass a certification exam administered by the NASA PKI Certification Authority; and

b. add, modify, restore, and delete Entrust PKI Certificates in accordance with Agency procedures.

6.11 Operational Support for IT Security

The HITTS contractor is responsible for management of the ITS function within the Headquarters' infrastructure including the Data Center and to coordinate observations of anomalous behavior, analysis of threats as well as threat responses with those in the ITS, network and HQ IT communities. (see ITS section 8.0). The contractor shall:

a. maintain a clear and complete understanding of all internal network protocols used and associated internal-to-internal and internal-to-external source(s)/destination(s);

b. maintain an escalation and analysis call list for all points-of-contact required in resolving ITS operations problems;

c. provide anomalous behavior analysis, status and reporting during Prime Time hours; and

d. collect and analyze threat alert information from the Security Operations Center, local Intrusion Detection systems (IDS), security scanners, vendor alters, hacker boards and others and provide recommendations for mitigation of IT Security threats (approximately 128 per month).

DRD	Description	Frequency
DRD #54	Intrusion Detection Summary.	One month after contract start date, monthly thereafter.

6.12 Physical Control Support

Because of the sensitivity of the systems and services within the Data Center, and because of the potential damage that could be done by an individual who has physical access to the hardware and network within it, the NASA HQ Data Center has restricted access which must be vigorously maintained by the HITTS contractor. The contractor shall:

a. monitor the physical security of the HQ Data Center and all sensitive unclassified automated information resources within the HQ Data Center;

b. work closely with HQ Security to control HQ Data Center access provided to contractor and subcontractor personnel;

c. comply with the policies and procedures for HQ Data Center physical security in accordance with established procedures; and

d. maintain server racks, server facilities and telecommunications closets in a clean, safe, and well organized way.

6.13 Environmental Control Support

The NASA HQ Facilities and Administrative Services Division (FASD) is primarily responsible for provisioning the environmental systems and power that support the HQ Data Center, however co-monitoring and coordination is critical to the safe operations of the HQ Data Center. The contractor shall continually monitor the environmental conditions of the HQ Data Center. The contractor shall immediately report all anomalous conditions to ITCD and to FASD. The contractor shall maintain a verified call and escalation list.

6.14 Technical Documentation and Data Center Reporting

The contractor shall develop, contribute, implement and/or update technical documentation for the HQ Data Center. Technical documentation shall include policies, operations, and guidelines. The contractor shall provide HQ Data Center System Assessment and Metrics Reports.

DRD	Description	Frequency
DRD #55	Data Center System Assessment & Recommendations Report.	90 days from contract start date, monthly thereafter.

6.15 Outage Notification

The contractor shall notify ITCD as early as possible of the need for outages or reduced services due to new security threats, investigation of anomalous behaviors, equipment failure, or other contingencies that cannot be scheduled. The contractor shall categorize activities as to whether they are security, equipment, service or software related on a 24/7 schedule and provide recommendations and take appropriate actions. If the anomaly is concluded to be equipment, service or software related, report to the performance monitor and take appropriate action(s) during normal working hours and within 3 hours for after hour occurrences

6.16 Printing Support

All printing support will be moved to the I^{3}P contracts. NASA HQ migrated 100% to /ip-based printing and away from print servers; therefore, there is only a minimal amount of work effort in this area. The exception is support for the PRGate print server which is in place to provision /ip printing across the HQ security zone for visitors using our guest wired and wireless network. NASA HQ does not anticipate a reversal to our elimination of print servers. To support printing the contractor shall:

a. assure timely and coordinated service upgrades on the remaining print server, PRGate; and

b. assure timely support and coordination for any security issues.

6.17 Video Teleconference Systems (ViTS) Support

The ViTS room operations team provides a full range of support services and technical expertise in support of point-to-point and multi-point video teleconferences at Headquarters. These services include the scheduling, conference consultation, conference setup, coordination with end points, and room operations. The contractor shall:

a. understand at an expert level the systems and components within the Headquarters ViTS rooms and ensure that all elements of the system are maintained in an operational and available state;
b. provide the scheduling function of the Headquarters ViTS rooms and coordination of conference setup with remote end points (approximately 36 per month);
c. assure staffing of rooms during video teleconferences and support services that include but not limited to room preparation, system and camera operation, recording, monitoring audio/video quality, and problem solving;
d. log attendance and customer satisfaction survey for each event; and
e. coordinate facility repairs and system maintenance as needed to ensure all elements of ViTS room services remain in an operational and available for use state.

7.0 Systems Engineering and Integration (SE&I)

The Systems Engineering & Integration (SE&I) function provides technical leadership in path finding, analysis, trouble-shooting and expertise in Information Technology, Information Security and Computer Science disciplines. As the technology leaders and lead analysts, the SE&I staff is tasked in areas of innovation, agency integration, systems design, requirements formulation and documentation, planning and to quickly resolve escalated problems.

The Systems Engineering & Integration support portfolio at NASA HQ is comprised of five areas of emphasis; (1) assurance that all new IT capabilities and services are designed and implemented in the most efficient and effective manner, (2) technical forecasting, studies conducted in areas that advance the goals of HQ IT, (3) participation in agency and external working groups, (4) advanced trouble shooting and problem resolution, and (5) HQ IT planning. There is an SE&I testing facility adjacent to the HQ Data Center and is specially purposed for testing, build-outs, vendor demonstrations and analysis (currently there are approximately 50 SE&I Service Requests initiated per year).

7.1 Innovation Program

NASA HQ customer's require agile adaption to organizational change or business needs. As a result, innovation must permeate all facets of this contract. To facilitate this requirement, ITCD has established an Innovation Program. To directly support this program, in conjunction with ITCD's CTO the contractor shall evaluate and investigate new and emerging applications technologies and approaches; and analyze and recommend technologies for integration and use within the NASA development and/or operational architecture. The contractor shall:

a. explain how specific new technologies can contribute to meeting ITCD's goals;

b. provide analysis of new and emerging applications technologies capabilities and maturity readiness;

c. analysis of alternative technologies (new or existing) that the ITCD should consider;

d. how a technology may fit into the NASA Enterprise Architecture;

e. analyze readiness factors for insertion of new technologies;

f. provide life cycle cost analysis for the proposed technologies;

g. provide technical demonstrations of evaluation packages; and

h. develop and maintain an online environment that provides details to innovative technologies and solution sets that aligns and conforms to similar systems at other centers.

DRD	Description	Frequency
DRD #56	Online Innovation Environment. Provide updates, align content so that it is searchable and at the accepted level of detail.	90 days from contract start date, monthly thereafter.

7.2 IT Service Design, Integration & Implementation

IT Services may include everything from migrating point to point data exchanges, to integrating multi-touch interfaces, to implementing rules engines to utilizing cloud algorithmic services. The contractor shall ensure that proposed implementations provide an integrated approach with respect to customer business needs, requirements, existing HQ IT infrastructure, future direction, IT Security, work in progress, and applicable NASA policies, standards, and methodologies. This integrated approach shall encompass the architecture, equipment, software and data associated with the HQ environment and driven by requirements and use cases. Occasionally, establishment, enhancement or extension of a service capability may include other NASA centers or customers outside of NASA HQ.

In order to align ITCD with the Agency's strategy for data centers, the contractor shall develop, submit and regularly update a Data Center Modernization Plan, detailing plans during the upcoming period and the top five to ten quantifiable objectives expected to be achieved. The Government and Contractor will discuss, modify (if necessary), and agree to the top five to ten objectives, which will form the basis for a portion of the incentive fee determination (technical performance) during that period. The contractor shall submit a report at the end of each period to describe the accomplishments against the objectives met from the previous period and which 5-10 objectives will be targeted for the next period. The Data Center Modernization Plans shall align with the general guidance in section 2.3.1 and 2.3.2 of this Performance Work Statement.

DRD	Description	Frequency
DRD #57	Data Center Modernization Plan	Two months from contract start date, and every six months thereafter.

7.2.1 System Engineering Requirements & Analysis

As the technical leads in several areas, it is critical that the SE&I requirements analysis documentation is valid, timely and complete. The SE&I requirements process will be in conformance with the EA/CCB guidelines. The contractor shall be responsible for:

a. the collection, interpretation, generation, validation and documentation of requirements for IT systems and services;

b. assurance that derived requirements are captured and documented;

c. requirements gathered and documented at a sufficient level of detail and in a form that is useful for the Government, or another Government contractor or used as part of analysis requested by a HQ customer;

d. annotation of requirements generated by another NASA, Government or vendor to depict relevance to the HQ IT infrastructure or point of view;

e. assessments to resolve near-term operational issues, implementation strategies, improve services, advance information management, reduce risks, reduce costs or to improve the customer experience; and

f. analysis, interpretation, studies regarding changes to technology, policy or lessons learned which may benefit or impact HQ IT customers, infrastructure, or plans.

7.3 Systems Engineering Design

Design solutions must meet or exceed use cases and address all requirements. The contractor shall be responsible for:

a. designs to meet the documented requirements;

b. designs consistent with Internet, Industry, Agency and / or HQ standards, architecture or design targets (e.g. High Availability);

c. designs consistent with rigorous application of design-to-cost methodology;

d. specifications for systems, components, equipment, and software, services, supplies and Concept of Operations (ConOps) that implement the design;

e. written documentation of all designs, in accordance with Industry, government or NASA HQ standards;

f. design coordination with the HQ IT Security, Operations, Applications, and other appropriate groups to ensure that risks are minimized and that security requirements are being adequately addressed and satisfied;

g. design reviews to ensure that a design meets documented requirements and architectural target, consideration of human factors (e.g. usability, training), engineering principles (e.g. minimizes security risks, and effectively and efficiently uses HQ and/or NASA IT resources); and

h. design and specification reviews that are in accordance with Configuration Control Board processes.

7.4 Systems Integration & Implementation

Assurance that designs of proposed solutions are made available and are supportable within our infrastructure demands thorough analysis and coordination. The contractor shall be responsible for:

a. a systems view, understanding the interdependencies between HQ, Center, contractor services, agency services, and Internet services;

b. implementations that provide an integrated approach with respect to existing HQ IT infrastructure, customer support, IT Security, other work in progress, and applicable NASA policies, standards, and methodologies;

c. implementations to enhance or extend a service or capability to HQ that is part of other NASA, government or business partners;

d. implementations to enhance or extend a service or capability within HQ, to other NASA Centers or to customers outside the Agency;

e. staying current with evolving systems designs and implementations to ensure integration with other NASA systems or services (e.g. I^3P, ITS, pilots, etc.); and

f. build out of new servers & services, installation applications, production servers support maintenance.

7.5 Forecasting, Studies and Development

The contractor shall maintain awareness of new trends in technologies, evolution in services, and developments in service delivery strategies that are emerging in academia, standards communities, Industry or Government at sufficient levels to recommend innovations and to determine applicability, readiness and impact. The driver is a continual assessment to identify opportunities to improve the provisioning of IT services, increase capability, decrease costs, and improve information services to the customer. The contractor shall:

a. provide assessments based on sound analysis to implement new capabilities that either advance ITCD’s stated direction or that are game-changing and warrant augmentation of target states;

b. provide path-finding and technical reviews that indicate important trending and areas to watch;

c. offer analysis, whitepapers, trending and similar products to stimulate possible direction or to elevate awareness of potential changes to HQ IT;

d. provide assessments of white papers, initiatives or the proceedings from working group sessions that are conducted under the auspices of the NASA Chief Information Officer (OCIO), conferences, and seminars;

e. conduct technology comparative analysis that evaluate emerging IT technologies and services that have not yet been introduced to the NASA or HQ IT environment to determine their applicability, feasibility, trade-offs and cost-benefit to HQ or the Agency’s mission, customer or project support requirements;

f. interview, participate and otherwise facilitate the collection of input from the Customer Advisory Committee and other stake holders to identify business needs and utilize them to develop the Tactical plan initiatives;

g. conduct analysis of customer and HQ IT business needs and draft the associated Tactical Plan initiatives to meet or address customer needs;

h. perform pre-release testing, (when approved by the CCB process) new monitoring, management, or operating systems, load balancers, network subsystems, video integration, nomenclature/metadata management, incomplete query, model-based planning and other tools supplied by contractors or available in open source;

i. provide reviews and assessments of working group activities within the auspices of the OCIO, standards, industry or government working groups or of conferences and workshops;

j. provide input to the development and update of the HQ Tactical Plan, Strategic Plan, or Integration Plans;

k. deliver each assessment as a written document or in HTML on a designated site using appropriate metadata; and

l. provide recommendations and update the Tactical Plan quarterly as conditions change or modifications or updates are made to Federal, Agency, or HQ regulations, policies, or strategic direction occurs.

DRD	Description	Frequency
DRD #58	HQ Tactical Plan.	Annual and updates as required.

Metric	Description	Performance Level to Achieve Fee
Metric #12	Delivery of Annual Tactical Plan and Quarterly Updates. Tactical Plan shall be fully documented and delivered annually after IT Board of Directors' approval; or Tactical Plan Status Report shall be provided quarterly to reflect current status and projections.	50% submitted on time.

7.6 Agency and External Support Initiatives

The contractor shall support in planning for and accomplishing the IT integration necessary to implement Agency initiatives at HQ. In some instances this support includes ensuring that cross-Center and cross-Agency systems work effectively and can exchange information while adhering to NASA IT security requirements. The contractor shall:

a. support in planning for and accomplishing the IT integration necessary to implement Agency initiatives at HQ;

b. ensure that cross-Center and cross-Agency systems work effectively and can exchange information while adhering to NASA IT security requirements;

c. provide assessments of security, performance, cost and process impacts that Agency initiatives may have on the NASA HQ infrastructure; and

d. support or consult in IT Security assessments and or penetration testing and in any required countermeasures.

7.7 Support OCIO and other projects, working groups

NASA programs and projects traverse many NASA Centers, often with Program leadership residing at HQ. From an IT perspective, HQ is an important participant in Agency OCIO activities to improve uniform capabilities across all of NASA. Achievement of these goals requires analysis of alternatives for governance, management and technology, often at working group levels or in fielding cross-center projects. The contractor shall:

a. participate in weekly/monthly Agency working group telecons and attend annual/semi-annual Agency Face-to-face meetings (approximately 20 working groups totally 100 labor dollars per month and support for 8 face-to-face meetings);

b. monitor and report working group activities;

c. track actions, scheduling and facilitating the preparation of responses;

d. consult with and debrief the HQ CIO and staff regarding impacts to budget, schedules, infrastructure and levels of effort;

e. support the provisioning of services by a NASA Center, another Federal agency, or a private entity to NASA HQ, or by NASA HQ to another organization;

e. coordinate seamlessly with external contractors in order to achieve successful implementation;

f. support in the development of extended and distributed service models;

g. draft memoranda of agreement / Memorandum of Understanding and Service Level Agreements and development of the online template DBMS entry; and

h. develop and document web-services or, if needed, point-to-point data exchange agreements.

7.7.1 HQ Support to Identity, Credential, Access Management (ICAM) and Supporting Systems Infrastructure

To conform to Federal regulations, NASA is taking steps to centrally control physical and IT resources in the areas of Identity, Credential, and Access Management (ICAM). This effort is being implemented through several related Agency-wide projects to track and validate identities, and to provide for centralized authentication and authorization for both physical and logical access to NASA resources. The Agency ICAM program is in direct support of Homeland Security Presidential Directive (HSPD) 12. It was renamed to better align integration of HSPD-12 with NASA business processes.

The Contractor shall act as a technical point of contact, and provide consulting, engineering, application development, communication and training, and sustaining operations support as needed for all ICAM-related projects, as well as new projects which may be started under the auspices of ICAM. Currently the following systems are within scope of ICAM:

- Common Badging and Access Control System (CBACS);

- Desktop Smart Card Integration (DSI);
- NASA Enterprise Physical Access Control System (EPACS);
- Identity Management and Account Exchange System (IdMAX);
- NASA Account Management System (NAMS);
- Two-Factor Token Infrastructure (TFTI);
- NASA Enterprise Directory (NED);
- NASA Consolidated Active Directory (NCAD).

7.8 Special Analyses, Studies, and Tasks

Subject to the issuance of service requests or tickets, the contractor shall conduct special studies and analyses addressing a variety of IT-related topics. Examples of support that the contractor may be called upon to provide include:

- updates to the Office of Diversity and Equal Opportunity Discrimination Complaints Management System to include new fields and reports as well as interactive features;
- action tracking systems that will allow HQ offices to capture, assign, and manage to completion actions generated both internally and received through official Agency channels;
- technical analyses of draft NASA and federal policy documents to determine their impact on NASA's IT capabilities and environment;
- analyses of life cycle documentation of systems developed/proposed by federal agencies for NASA's use to determine adequacy of requirements, design, security considerations, etc.;
- analyses and studies to support NASA HQ in complying with Section 508 of the Rehabilitation Act, the Privacy Act, the Federal Information Security Management Act, Homeland Security Presidential Directive-12 (HSPD-12), and other IT-related directives, statutes, and implementing regulations;
- tracking, analyses, and compilation of information on IT security bulletins issued by the U.S. Computer Emergency Response Team (US-CERT) and other organizations.

7.9 Advanced Trouble Shooting & Problem Resolution

The contractor shall provide engineering support for the operations, maintenance and enhancement of all NASA HQ IT infrastructure, applications and services and function as a centralized capability for escalation of technical issues. The contractor shall:

a. provide support to resolve issues with the design, installation, configuration, testing, securing, upgrade, or diagnoses of problems with computer room, network, application, and security assets;

b. provide support to resolve issues locally that may be part of agency or government-wide solutions;

c. respond promptly to requests for trouble shooting and resolution; and
d. recommend methodologies to proactively model systems to determine if a problem is likely to occur.

7.10 IT Planning

Planning activities include assuring that business drivers and requirements are in alignment with process change and IT service implementation. Structured planning is essential in several areas for HQ IT (e.g. agency integration, reaction to changes in organizational roles, changes to policy, threats, technology, and more fundamental changes in how services are provisioned or capabilities introduced. The contractor shall:

a. participate in the development of HQ IT Tactical, Strategic and budget planning
b. develop a resourced schedule and integrated plan that will guide HQ in completing NASA strategic IT initiatives;
c. assure alignment with NASA's Information Resource Management (IRM) Strategic Plan, Open Government Initiatives and similar external drivers;
d. assure alignment of requirements to implementation and solution to business driver by Enterprise Architecture techniques; and
e. assure alignment to Agency's and HQ IT Capital Planning and Investment Processes.

7.11 IT Systems Engineering & Integration Test Lab

The contractor shall maintain and operate the HQ IT Systems Engineering and Integration Test Lab. The lab is used to replicate the HQ infrastructure sufficiently for testing and acceptance of new services, evaluations of potential services (prototypes and proofs-of-concepts), build-outs, vendor testing, and debugging. A staging area of the lab with specialized network policy is used for pre-deployment testing and checkout of applications, services, or new operating systems. Because changes to form, fit or function of the HQ infrastructure is not permitted without thorough testing and approval by the CCB, the maintenance and currency of the lab is critical to assure sufficient simulation of the HQ IT service infrastructure. The contractor shall be responsible for applying technologies in support of customer tasks encompassing deployment of web, multimedia, or virtual environments, maintaining optimum configuration controls, scheduling individuals, and support to ensure that the correct hardware and software is on hand. The lab is staffed to facilitate setups, tear downs, support for engineering, developers, vendors and HQ customers. To sustain and operate the IT test lab the contractor shall:

a. maintain a log of tests that occurred with results;
b. maintain a schedule of testing required (approximately 37 instances of testing per month);
c. assure testing assets are ready and available prior to scheduled tests;
d. maintain detailed knowledge of the HQ production environments (e.g. workstations, servers, networks, and security);

e. maintain a detail knowledge of potential agency environments required for simulation;

f. document and assess the impact or risk of any areas that cannot be simulated and their effect on the testing conducted;

g. assure and document the as-built and build out of lab service infrastructure in support of simulating test environments;

h. validate test plans;

i. maintain, operate and coordinate the SE&I Test Lab's network, connectivity, firewalls, IDS, monitoring and staging in accordance with HQ and agency security policy and operational procedures and assure that production data is controlled and limited to the pre-production/staging segment of the lab; and

j. manage, coordinate, trouble-shoot and otherwise ensure operational stability between the SE&I Test Lab and the HQ network service provider.

DRD	Description	Frequency
DRD #59	Systems Engineering & Integration Test Lab Performance Report.	Two months from contract start date, continuously available thereafter.

8.0 IT Security (ITS) Program

Protecting the Nation's intellectual and computational assets, NASA's information, our customer's privacy, and our ability to perform work without interruption are all critical goals for our IT Security team. Our commitment and emphasis in IT Security is integrated in all of our processes including prevention, recovery, compliance, and analysis. This emphasis extends to our internal systems, the contractor's environment, and external systems accessed by our customers. ITS planning, implementation, and compliance is integral to all work performed under this contract, and therefore is not limited to the contractor's IT security staff. The contractor is responsible for ensuring that all of the services it provides complies with Federal law as well as Agency and HQ policies, processes, procedures, regulations, requirements, and standards. The contractor is also responsible for providing technical and managerial support for the HQ ITS Program, which is under the direction of the HQ IT Security Manager (ITSM). The Contractor shall document their approach to managing information security in an Information Security Management Plan to be delivered within one month from contract date. This plan shall be reviewed and updated at least annually.

DRD	Description	Frequency
DRD #60	Contractor Information Security Management Plan.	Within one month from contract start date, updated annually thereafter.

8.1 Contractor Support for Headquarters ITS Program

The contractor shall provide comprehensive ITS support to the HQ ITSM. The activities associated with this support are those for implementing the policies, processes, procedures and guidelines of Federal Information Security Management Act (FISMA), the Computer Security Act of 1987, OMB Circular A-130, NPR 2810.1, NPR 1600.1, NIST Special Publications and Federal Information Processing Standards (FIPS), and other Agency/HQ policies, processes, procedures and guidelines governing the protection of information resources. The following are specific security support requirements that enhance selected governing security items.

8.1.2 Standards and Procedures

The contractor shall develop and maintain security standards and procedures for a broad range of IT operations and support in accordance with Federal and NASA policies, requirements, and guidelines. Categories include, but are not limited to:

- System access controls;
- Account management controls;
- Technical, network, and environmental security controls;
- Risk management;
- Information System Security Authorization (ISSA)
- Virus detection and eradication;
- Encryption
- Vulnerability monitoring and scanning;
- Penetration testing;
- Remote access;
- Secure communications;
- Security monitoring;
- Personnel screening procedures;
- Incident handling response and reporting controls;
- Contingency planning;
- Application development security controls; and
- Auditing metrics.

8.1.3 HQ Draft Policy, Requirements, Procedure, and Standards Development

The contractor, when tasked by the HQ ITSMs, shall develop draft NASA HQ policies, requirements, and procedures for review and approval through established HQ procedures.

Documents shall be accurate, complete, professional, and tailored for audiences inclusive of non-ITS personnel.

DRD	Description	Frequency
DRD #61	Draft Policy, Requirement, Procedure, or Standard.	In accordance with accepted SOP updates.

8.1.4 Support of ITS Program Meetings

The contractor shall provide the HQ ITSM schedules and status of completed, current, and future ITS program projects on a bi-weekly basis. The contractor ITS program lead, or designated alternate, shall attend Agency ITS teleconferences and off-site NASA ITS working group meetings as required.

8.1.5 Security Configuration Baseline Documents

In accordance with CCB approval, the contractor shall develop and maintain security configuration baseline documents. These baseline documents shall provide additional security control configuration details beyond the documented security settings that are required under NPR 2810.1 or other HQ policies or guidelines; i. e., they shall specify security controls in effect for each of the following HQ supported items:

- Operating systems;
- Personal Digital Assistant (PDA) operating systems;
- Email clients;
- Web browsers; and
- Publicly accessible NASA HQ Library systems (desktop operating system only).

8.1.6 Freedom Of Information Act (FOIA), General Counsel, and Congressional Requests

Upon request, the contractor ITS team shall download and parse user e-mail data from NOMAD (NASA's Operational Messaging and Directory) email service, Tivoli backups of users, or copies of user e-mail files. If no NOMAD or Tivoli files are available, the ITS team will contact the user and arrange to copy their mailbox from their workstation. The contractor ITS team shall electronically search the records based on criteria provided through the HQ ITSM using Paraben E-Mail Examiner or similar software. The contractor shall develop an index for the data. The contractor shall load the index and all data meeting the criteria to appropriate removable media (CD-ROM, DVD, Thumb Drive, etc) and provide at least two (2) copies to the requesting ITSM for delivery to the customer.

DRD	Description	Frequency
DRD #62	eMail Data Search Results.	On demand.

8.1.7 Human Resources and Inspector General Requests

The contractor ITS team shall conduct forensic imaging of user workstations in support of HR appropriate use investigations and IG criminal investigations. Data collection may need to occur after normal business hours when the subject and other area personnel are not present. HR requests will usually include analysis of data to identify and capture evidence of inappropriate use of HQ IT resources. IG investigations will usually only require acquisition of data and provide it to the IG Computer Crimes Section for analysis and investigation.

8.2 Security requirements for Contractor Provided Services

The contractor shall develop and document management, operational, and technical ITS procedures and controls for all services the contractor provides to NASA HQ. For each of these services, the contractor shall:

a. integrate the ITS procedures and control measures into their full life cycle;
b. test and periodically review procedures and controls for adequacy and compliance;
c. allow NASA access to the contractor's and sub-contractor's facilities, installations, technical capabilities, operations, documentation, records, databases and personnel to the extent required to carry out a program of ITS inspection and audit. This access is needed to safeguard against threats and hazards to the integrity, availability and confidentiality of NASA data;
d. not store, copy, or transfer NASA confidential, Sensitive but Unclassified (SBU), or production data across non-production or development systems and networks, including off-site support systems and networks;
e. encrypt all electronic data transmissions of risks, threats, and/or vulnerabilities;
f. for all contractor IT systems storing, containing, or otherwise processing Federal or NASA information be certified and approved to operate storing government information in accordance with Federal and NASA regulations. Hard copy sensitive information and portable electronic devices will be stored and protected in accordance with Federal and NASA regulations;
g. maintain separation of sensitive IT duties to limit risks require two individuals to access password storage facilities. (e.g. different individuals perform information system support functions for system management, systems programming, configuration management, quality assurance and testing, network security and personnel who administer access control functions do not administer audit functions); and
h. provide copies of contractor systems with eight business hours upon request for normal requests, the contractor shall provide to the COTR a full, bit-by-bit copy of any system they use to support NASA HQ. For urgent requests, the copy shall be provided within two business hours. This shall be completed using forensically sound software capable of providing image hashing. The copy shall be delivered on media appropriate for the amount of data. The authority to obtain such data is provided by NPD 2540.1G, Personal Use of Government Office Equipment including IT; and the NASA Headquarters Appropriate Use Policy.

8.2.1 Compliance with Regulation and Policy

The contractor shall ensure adherence to all of the relevant Federal, Agency and HQ regulations, policies and procedures in the execution of their duties in support of NASA. The contractor shall;

a. ensure that all US Government information provided, developed, or acquired under this contract is properly secured in accordance with Federal and NASA Requirements including but not limited to NPR 1600.1, NPR 2810.1A, NITR's, NASA ITS Handbooks, and other OCIO, NASA Office of Protective Services, and NASA HQ requirements;
b. adhere to applicable policy directives (e.g. NASA Procedural Requirements (NPR) 2810.1A Security of Information Technology; NPR 1600.1 NASA Security Program Procedural Requirements; NASA Policy Directive (NPD) 2540.1G, Personal Use of Government Office Equipment Including IT; NASA Federal Acquisition Regulations (FAR) Supplement 1852.204-76; National Institute of Standards and Technology (NIST) Special Publications (SP) – 800 Series and Federal Information Processing Standards (FIPS); NASA Information Technology Requirements (NITR); NASA ITS Handbooks; NASA Agency Chief Information Officer (CIO) requirements; HQ policies and procedures; and other governing security items); and
c. adhere to applicable system & application life cycle requirements including the NIST Guide for Assessing the Security Controls in Federal Information Systems and Organizations, NIST SP 800-53A, Rev1, NIST Risk Management Guide for Information Technology Systems, NIST SP 800-30, and the HQ Security Review Process requirements during all phases of the System and Application Life Cycle.

8.2.2 Privileged and Limited Privileged Access

The contractor shall follow NPR 1600.1, NASA IT Requirement (NITR)-2810-14A, Managing Elevated User Privileges on NASA IT Devices, NASA ITS-HBK-0004, Managed Elevated Privileges Implementation Guidance Handbook, and the Headquarters Contractor Badging and Screening Process. All contractor requests for privileged or limited privileged access shall:

a. be made a minimum of six week prior to need date;
b. request approval from the HQ Center Chief of Security through the NASA COTR in the event the contractor needs to provide privileged or limited privileged access to one of their employees who do not meet the requirements stated in NPR 1600.1;
c. not fill positions with, or assign duties that require privileged or limited privileged access to foreign nationals regardless of status; and
d. document in a monthly report all privileged and limited privileged positions and current

DRD	Description	Frequency
DRD #63	Monthly Privileged Position Report.	Within one month from contract start date, monthly thereafter.

8.3 Security Risk Assessments and Design Reviews

NASA relies on the ITS staff to assure that new systems, services and contexts are safe and do not introduce new threats or weaknesses into our environment. The contractor shall:

a. ensure that system data categorization occurs prior to System/Software Requirements Review (SRR);
b. complete a preliminary security risk assessment on a design prior to the Critical Design Review (CDR);
c. provide design security risks, including possible mitigations, to the line manager or equivalent, data owner, and application owner prior or during official design review. If the risks are accepted the life cycle may continue, otherwise the life cycle shall cease or the design and/or mitigations shall be modified until the risks and possible mitigations are acceptable; and
d. ensure that the system security plan and risk assessment are completed and/or updated, as applicable, prior to Operational Readiness Review (ORR) (all risks must be accepted by the application and system owner prior to ORR).

8.3.1 Security Reviews and Assessments for New or Modified Hardware and Software

The contractor shall conduct a security assessment for all new hardware products introduced on an HQ system. The review shall include research to identify all known vulnerabilities for the product. The assessment shall identify all risks associated with product and recommend mitigation actions. The review shall also ensure that the product complies with the appropriate security configuration baseline. If none exists the ITS team shall also develop one for the product. Completed reviews will be forwarded to the HQ ITSM and system owner for approval. Approved reviews will be forwarded to the contractor ITS ISSA Team lead for incorporation into the appropriate ITS plan(s). The contractor shall ensure that security is practiced throughout the system life cycle for all hardware, software, and supplications managed by the contractor. The contractor shall conduct security reviews and risk assessments for HQ custom applications, new or updated hardware, and new or updated commercial-off-the-shelf (COTS) software products. The contractor shall:

a. provide the system owner a written risk assessment and security review for new or significantly modified HQ hardware or software, prior to deployment;

b. use the products reviewed as a basis to update ITS Plans, as applicable;

c. present to the system owner, prior to deployment, all risks and recommended mitigations (separate from the security plan) for approval. If the hardware or software connects to other systems, the approved risks and mitigations shall also be presented to the system owners of the interconnected systems for their information;

d. on an ad hoc basis, the contractor shall provide written risk assessments and technical security reviews as requested by the HQ ITSM or NASA COTR. The assessments and reviews developed shall be used as a baseline to update ITS Plans, as applicable. All risks shall be presented to the line manager or equivalent, at least verbally, and subsequently reflected in the applicable security plan. If the system connects to other systems, the risk assessment shall also be presented to each interconnected line manager or equivalent;

e. conduct a security review for all new COTS software products prior to their installation on an HQ operational system component in accordance with the NASA HQ Triage 3 SOP (approximately 13 per month). Completed reviews will be forwarded to the HQ ITSM and system owner for approval. Approved reviews will be forwarded to the contractor ITS ISSA Team lead for incorporation into the appropriate ITS plan(s);

f. conduct a security review for all new HQ custom applications and application changes developed by the contractor applications development team or developed by others for deployment on HQ systems. Reviews shall follow the NASA HQ Security Review SOP. Completed reviews will be forwarded to the HQ ITSM and system owner for approval. Approved reviews will be forwarded to the Application owner, Application Development Team, HQ Software Applications Manager, and the contractor ITS ISSA team lead;

g. review annually IDS signatures and firewall rule sets to determine their validity in relation to services provided and associated risks. The results of the review shall be documented, including a description of updates implemented; and

h. ensure that all systems operated or maintained are compliant with Federal Desktop Computer Controls (FDCC), Center for Internet Security (CIS) Controls, or controls specified in the NASA security configuration baseline documents as applicable.

These baseline documents provide additional security control configuration details beyond the documented security settings that are required under NPR 2810.1 or other HQ policies and guidelines. They specify security controls in effect for each of the following supported items:

- Operating systems;
- Personal Digital Assistant (PDA) operating systems;
- Email clients;
- Web browsers; and
- Publicly accessible NASA HQ Library systems (desktop operating system only).

The contractor shall only deploy, into production, hardware and software, including security related patches or upgrades, which have been subject to a NASA-approved security review.

DRD	Description	Frequency
DRD #64	Security Reviews and Assessments.	On demand.

8.3.2 IT Vulnerability Management, Scanning and Monitoring

The contractor shall manage and monitor IT vulnerabilities in accordance with NPR 2810.1A and NITR-2810-24, *NASA IT Device Vulnerability Management*. The contractor shall:

a. conduct and document vulnerability scanning and monitoring, required of each NASA Center, in accordance with NPR 2810.1A and NITR-2810-24 and other guidance provided by the Agency;

b. use the NASA approved tools and profiles;

c. provide ITS vulnerability services each business day by monitoring/reviewing the following:

    - Foundstone vulnerability scans,
    - Patchlink Critical and Critical-01 ratings,
    - NASA SOC distributed bulletins and alerts,
    - US CERT bulletins and alerts,
    - NIST distributed bulletins and alerts,
    - The HQ standard web browser contractor web sites,
    - The HQ standard email client web site,
    - The operating system web sites for all HQ system platforms,
    - Vulnerability scans,
    - Relevant emails from the HQ ITSM.

d. conduct and document monthly vulnerability scans of all NASA HQ owned IP addresses using the NASA approved vulnerability scanning tool and HQ scanning profiles. The results of the HQ tests shall be documented in a monthly report provided to the HQ ITSM. All vulnerabilities found during scanning shall be assessed and distributed per the Vulnerability Reporting and Monitoring section;

e. conduct monthly analog telephone scanning to verify that no unauthorized analog lines are connected to NASA HQ computers;

f. submit a monthly report indicating identity of any unauthorized analog lines shall be submitted, even if no unauthorized analog lines are detected;

g. conduct monthly wireless 802.11 scanning to verify that no unauthorized wireless systems are connected to the NASA HQ wireless network;

h. submit a monthly report identifying all detected authorized and all detected unauthorized wireless system;

i. conduct ongoing continuous monitoring to detect rogue Bluetooth devices and ensure configuration compliance of authorized devices;

j. conduct security scans of incoming devices (laptops, thumb drives, or other removable media, etc) to determine whether they meet Agency and HQ requirements for connection to our private network or insertion into devices attached to our private network. These devices may belong to other contractors supporting NASA HQ or NASA issued devices from another Center. Scans will generally be infrequent but may need to be conducted on short notice;

k. report to the HQ CERT, within four business hours after discovery, all unexplained system anomalies found while conducting normal duties that effect confidentiality of data or integrity of a system or data;

l. report to the Help Desk, all deviations of the HQ Appropriate Use Policy that are observed while conducting normal duties. If an observed deviation is thought to be a malicious activity that affects integrity, confidentiality or availability, it shall be considered a Computer Security Incident and immediately reported to the Help Desk; and

m. attend all weekly Agency working group meetings and periodic workshops and training related to scanning and monitoring and keep the ITSMs informed of issues and activities.

When the contractor identifies a vulnerability affecting a HQ system component, it shall be added to the Daily Risk Assessment Report. This report shall be distributed encrypted daily to the ITSMs, system owners, and system administrators of HQ systems. The intent of this report is to give system owners and administrators "early warning" of new vulnerabilities and patches that there systems will be required to incorporate. See section 7.1.9 Vulnerability Mitigation for more information.

DRD	Description	Frequency
DRD #65	Daily Risk Vulnerability Report.	Daily.
DRD #66	Monthly Vulnerability Scan Report (encrypted).	One month after contract start date, monthly thereafter.
DRD #67	Monthly Analog Telephone Scanning Report (encrypted).	Two months after contract start date, monthly thereafter.
DRD #68	Monthly Wireless 802.11 Scanning Report (encrypted).	One month after contract start date, monthly thereafter.

8.3.3 HQ Penetration Testing

The contractor shall conduct annual HQ penetration testing. These tests may include attack simulations, running automated scanning tools, or conducting physical inspections. The scope of the annual test shall be agreed upon annually in conjunction with the HQ ITSMs and HQ system owners. The contractor shall:

a. prepare proposed Rules of Engagement, Penetration Test Plan, and a comprehensive schedule outlining activities and anticipated man hours for approval prior to beginning the test;

b. provide daily status of test activities and findings to the HQ ITSM; and

c. Prepare a comprehensive Test Report describing the penetration test, methods, results, vulnerabilities, and recommendations for corrective actions and improvements to the NASA HQ ITSM, System Owners, and ITCD Management.

DRD	Description	Frequency
DRD #69	Annual Penetration Test Plan and Rules of Engagement and Schedule.	Annually by fiscal year's end.
DRD #70	Annual HQ Penetration Testing Report.	Annually by fiscal year's end.

8.3.4 Information System Security Authorization (ISSA) Documentation

The Federal Information Systems Management Act (FISMA) requires all Federal organizations to assure that systems are appropriately classified and the measures to secure them are adequate. The contractor shall follow the accepted process for monitoring, analysis, recommending and provisioning risk-based acceptance criteria as directed by the Government.

8.3.4.1 NASA Internal Systems

In support of the ISSA process for NASA Internal Systems, the contractor shall:

a. develop and maintain ISSA documentation for all internal HQ systems as required under NPR 2810.1A and Federal Regulations;

b. assist NASA system and data owners in categorizing systems as well as defining system hardware/software, system boundaries, system interconnections, system responsible officials, and system users;

c. analyze the system and provide security control recommendations to the system owner in accordance with NIST SP 800-53 guidance. The contractor shall document all security controls compliance for each system;

d. conduct a controls assessment in accordance with NIST SP 800-53A guidance and develop and maintain a Plan of Actions and Milestones (POA&M) for all identified risks in coordination with the system owner and operating officials;

e. conduct certification activities for all HQ Internal systems categorized at the low level in accordance with Federal and NASA requirements;

f. coordinate all certification activities, as required, for all systems categorized at the Moderate and high levels;

g. conduct and document an annual controls assessment as required by NASA and Federal regulations; and

h. update ISSA documentation as changes occur affecting the security of a system

i. load and maintain all ISSA documentation in the NASA Security Assessment & Authorization Repository (NSAAR).

8.3.4.2 NASA External Systems

In support of the ISSA process for NASA External Systems, the contractor shall:

a. support, or fully develop and maintain ISSA documentation for NASA HQ external systems at outside agencies, contractors, universities, or other organizations. The extent of involvement will be decided on a case-by-case basis;

b. support NASA external system owner, information owner, and accountable official (i.e. NASA authorizing official) in categorizing systems as well as defining system hardware/software, system boundaries, system interconnections, system responsible officials, and system users. The extent of involvement will be decided on a case-by-case basis;

c. analyze the system and provide security control recommendations to the NASA External System owner in accordance with NASA, NIST SP 800-37 and NIST SP 800-53 guidance. The contractor shall document all security controls compliance for each system as required. The extent of involvement will be decided on a case-by-case basis;

d. conduct a controls assessment in accordance with NASA and NIST SP 800-53A guidance and develop and maintain a Plan of Actions and Milestones (POA&M) for all identified risks in coordination with the NASA External System Owner and Contractor system operating officials. The extent of involvement will be decided on a case-by-case basis;

e. conduct certification activities for HQ External Systems in accordance with Federal and NASA requirements;

f. conduct, document and provision for continuous monitoring of information security controls as required by NASA and Federal regulations; and

g. load and maintain all ISSA documentation in the NASA Security Assessment & Authorization Repository (NSAAR).

Contractor personnel involved with external systems may be required to sign non-disclosure agreements prior to commencing any ISSA activities.

8.3.4.3 Coordinate Risk and POA&M Updates

Prior to each meeting of the HQ Configuration Control Board (CCB), the contractor ITS personnel shall meet with each internal and external system owner (as required) to review system security reviews and mitigation recommendations for the purpose of gaining concurrence. The contractor shall on a monthly basis, coordinate, prepare, and provide an updated POA&M Status Report to the HQ ITSM that reflects the status of each POA&M item for each internal and external system. On a monthly basis, the contractor shall also coordinate, prepare, and provide an ISSA Status Report to the HQ ITSM that includes an update of all ISSA activities that occurred in the last month.

DRD	Description	Frequency
DRD #71	IT C&A Security Plan Assessment using the NASA standard template.	Annually by fiscal year's end.
DRD #72	Risk Assessment.	Annually by fiscal year's end.
DRD #73	Security Controls Assessment Report Assessment using the NASA standard template.	Annually by fiscal year's end.
DRD #74	Plan of Actions and Milestones Assessment using the NASA standard template.	Annually by fiscal year's end.
DRD #75	System Certification Report.	Annually by fiscal year's end.

DRD #76	Monthly POA&M Status Report.	One month after contract start date, monthly thereafter.
DRD #77	Monthly ISSA Status Report.	Two months after contract start date, monthly thereafter.

8.4 Vulnerability Mitigation

The ITS program is responsible for mitigation, response and preventive measures. System vulnerabilities are required to be mitigated in a timely manner. Mitigations shall occur in accordance with the most current NPR 2810.1 and NITR 2810-24, NASA IT Vulnerability Management. Depending on the assessed severity (critical escalated, critical, high, medium, or low) of a vulnerability and NASA System Owner concurrence with the severity, the contractor shall evaluate, test, and implement mitigation. The contractor shall notify the NASA System Owner when vulnerabilities are mitigated. A permanent mitigation is required for an expedited, critical or a high vulnerability. In some cases a temporary mitigation may be necessary. The contractor shall obtain approval by the NASA System Owner for a temporary mitigation. For a medium or low vulnerability, the contractor may mitigate the vulnerability or present a thoroughly researched recommendation that justifies accepting the risk. The contractor shall comply with the standard and expedited requirements in the Vulnerability Mitigation Requirements Table below. The contractor shall obtain approval by the NASA System Owner for any deviation from the requirements. In some rare circumstances, the NASA Deputy CIO for ITS, the NASA HQ CIO, or their designees may determine that a particular patch must be applied more urgently. In such cases, all information systems shall be patched in the timeframe specified.

Metric	Description	Performance Level to Achieve Fee
Metric #13	Vulnerability Mitigation. All system vulnerabilities shall be mitigated within the specified times, based on the assessed severity.	95% - 97% meet the criteria.

8.4.1 Incident Response

The contractor shall:

a. staff and operate the NASA HQ Computer Emergency Response Team (CERT) to respond to computer incidents in accordance with the NASA HQ Incident Response SOP (approximately 46 per month);

b. during Prime Time hours of 6:00 am until 6:00 pm Monday through Friday, except for holidays, support the identification and mitigation of incidents. During non-Prime Time hours respond to a phone call, a NASA Security Operations Center (SOC) or NASA Help Desk notification, or other Government notification within 15 minutes and arrive on-site, if necessary, within two hours of the initial notification;

c. conduct a daily review of the SOC Daily Reports, SOC Incident Tickets, HQ Antivirus Daily Reports, Content Filter logs and conduct further investigations as appropriate;

d. follow the HQ Incident Response Process and document all incidents in the NASA SOC Incident Management System (IMS);

e. ensure that all SOC incident tickets are processed and closed in a timely manner; and

f. annually conduct incident response training and conduct an incident response exercise in accordance with the NASA HQ Incident Response SOP.

DRD	Description	Frequency
DRD #78	Incident Response Training and Test Report.	Annually by fiscal year's end.

Metric	Description	Performance Level to Achieve Fee
Metric #14	Incident Response. During non-Prime Time hours respond to a phone call, a NASA Security Operations Center (SOC) or NASA Help Desk notification, or other Government notification within 15 minutes and arrive on-site, if necessary, within two hours of the initial page.	Meet the criteria 90% - 95% of the time.

8.4.2 Incident Reporting

The contractor shall immediately report to the HQ Computer Emergency Response Team (CERT) any known malicious activity or other suspected incidents that negatively affects the confidentiality, integrity or availability of HQ IT resources. The contractor shall immediately report all losses of IT devices, electronic media, or NASA information in accordance with Agency and HQ requirements.

8.4.3 Computer Sanitization

The contractor shall develop and implement procedures that ensure IT resources leaving control of an assigned user (e.g., the resource is being reassigned, repaired, replaced or excessed) have all NASA data and sensitive application software removed by a NASA approved technique. Applications acquired via a “site license” or “server license” shall be removed prior to resources leaving the control of NASA. Damaged IT storage media for which data recovery is not possible shall be degaussed by a NASA approved technique or destroyed. All sanitization shall meet the requirements of NPR 2810.1A; NITR 2810-22, *Media Protection Policies and Procedures;* and NASA ITS-HBK-035, *Digital Media Sanitization*.

8.4.4 Computer Anti-Virus Services

The contractor shall provide and properly configure anti-virus software on all workstations and servers. The anti-virus signatures on all systems shall be maintained and updated to the latest signatures as made available by the anti-virus software vendor. The contractor anti-virus server shall, at a minimum make available for distribution to client workstations and servers, updates to anti-virus signature files within two hours of vendor release. The contractor shall ensure that updates to anti-virus signature files are distributed to and activated on all client workstations and servers within eight hours of vendor release.

8.4.5 PKI Encryption Technical Support

The contractor shall provide engineering and technical support for HQ PKI Encryption technology. The contractor shall maintain and update the HQ PKI Registration Authority workstations as required. The contractor shall attend all NASA PKI Technical Working Group meetings and keep the HQ PKI Program Manager apprised of technical issues, changes, and upgrades. The contractor will work with the HQ Desktop Support contractor and the NASA PKI Technical Support to ensure that contractor supplied workstations have current NASA PKI software installed and operational.

8.4.6 Account Establishment and Termination Process

The contractor shall follow the HQ process for requesting, establishing, issuing and closing user accounts and authentication devices, including removal of user accounts after contractor employees depart.

8.4.7 Security Training

The contractor shall:

a. ensure all newly hired employees with access to NASA information resources complete NASA ITS Awareness Training within one month of start date;

b. ensure all of its employees, including sub-contractors with access to NASA information resources, complete NASA Annual ITS Awareness Training;

c. support, as required, the development and presentation of NASA Annual ITS Awareness Training for NASA HQ IT users;

d. employ an effective method for ensuring that all of its new employees, including sub-contractors, understand ITS policies and guidance provided by the ITSM and/or CIO as part of the new employee briefing process; and

e. ensure that all employees with system elevated privileges (1) possess requisite ITS skills in the operating systems they support; and (2) complete NASA elevated privileges training as required by NITR-2810-14A, *Managing Elevated Privileges on NASA IT Devices* and NASA ITS-HBK-0004, *Managed Elevated Privileges Implementation Guidance Handbook.*

8.5 Classified Work Requirements

Specific work performed by the contractor will require some individuals access to classified information, work in a secure area, or both, up to the level of Top Secret/ Secure Compartmented Information (TS/SCI). This work may include requests to assist NASA's Office of Protective Services (OPS) with classified system (e.g. providing technical support) or to collaborate with the intelligence community within NASA and other federal agencies specific to the details of an IT security incidents of a classified nature (e.g. forensics support). See Federal Acquisition Regulation clause 52.204-2 in this contract and DD Form 254, Contract Security Classification Specification. The Contractor shall ensure that key Contractor ITS personnel have the appropriate security clearances, up to the level of TS/SCI, to receive classified ITS threat information, to implement security controls based on such information, or to support other activities that require access to classified information.

8.5.1 ITCD Communications Security Support and Services

The Contractor shall provide COMSEC support and services to NASA HQ, acting as the HQ COMSEC Account Manager (CAM). Contractor COMSEC personnel shall possess and maintain a current TS/SCI level clearance preferably adjudicated within the last 36 months. In general, the contractor shall:

a. obtain, purchase, receive, safeguard, issue, provision accounting for, ship, and destroy (as required) all COMSEC material and equipment within the NASA HQ COMSEC account in accordance with Federal and NASA regulations and guidelines;
b. install COMSEC equipment, software, and keying material; troubleshoot COMSEC related user, equipment, and software problems; and conduct COMSEC user training and security briefings;
c. conduct HQ-wide COMSEC inspections and inventories consistent with National and NASA COMSEC policy and provide reports to the NASA HQ Information Technology Security Manager;
d. maintain currency and proficiency on National and NASA COMSEC policies and secure communications equipment;
e. coordinate with the NASA COMSEC Office of Record (COR) on COMSEC matters in support of the COMSEC function;
f. ensure availability for services within an agreed to schedule;
g. ensure a secure work environment inclusive of restricting unauthorized access to the COMSEC manager's material or work area; and
h. attend required training, working group meetings and similar authorized COMSEC events.

DRD	Description	Frequency
DRD #79	Quarterly Metric Report summarizing the transaction history, incidents, and inventories/inspections for that report	Due 90 days from contract start, and every 3 months thereafter

8.6 IT Service Continuity Management (ITSCM)

The contractor shall support the overall NASA ITSCM process by ensuring that required IT technical and service facilities (including computer systems, networks, applications, data repositories, telecommunications, environment, and technical support) operated by the contractor and supporting NASA HQ (and other NASA facilities as applicable) can be resumed within required business timeframes. The Contractor shall be responsible for developing, implementing, and providing ITSCM procedures that align with Government and NASA ITSCM Processes to mitigate the impact of a disaster or major failure. Plans, procedures and processes include Business Continuity Plans, Disaster Recovery Plans, Information System Contingency Plans, etc. developed in coordination with NASA HQ and other contractors providing IT and other support to NASA HQ. The contractor shall:

a. annually update, maintain, and test the HQ ITS Contingency Plan in accordance with NPR 2810.1 and NIST guidelines;

b. at least annually train contingency teams in plan procedures and operations;

c. at least annually develop, plan, and implement a contingency scenario test designed to validate the effectiveness of the plan to quickly restore HQ IT operations in the event of a disaster; and

d. deliver a lessons learned report from each test and use the results to update the HQ ITS Contingency Plan.

DRD	Description	Frequency
DRD #80	HQ ITS Contingency & Continuity Plan, Training and Test Report annual update	annually by fiscal year’s end

8.6.1 Disaster Recovery and Continuity Planning

The contractor shall support NASA in developing and testing plans to ensure continuous availability of IT systems and services at systems located at HQ and also for systems located at other Centers. The contractor shall:

a. support NASA in analyzing and providing comments and suggestions to NASA on the disaster recovery and continuity planning for systems operated by other Federal agencies and by commercial suppliers who provide services to NASA;

b. coordinate with information systems and disaster recovery experts across NASA and NASA's partners to verify integration of procedures and planning techniques for disaster recovery and continuity planning; and

c. support NASA in Agency-wide emergency preparedness and continuity of operations planning (COOP).

8.6.2 Emergency Operation Center (EOC) and Continuity of Operation (COOP) support.

The NASA HQ EOC, located at 300 E St SW, consists of workstations, printers, monitors, PA system and network connections. In an emergency, EOC personnel meet in the room to implement necessary actions. Emergency exercises are conducted in the EOC on a regular basis. Recovery exercises at the remote failover site will be conducted twice a year. The contractor shall provide IT support for the EOC room when needed and during real emergencies. The contractor shall recommend improvements after each recovery exercise and shall implement improvements only after receiving approval by the COTR or designee. In addition to an EOC room, NASA HQ maintains COOP sites at Goddard Space Flight Center, Langley Research Center, and the Glenn Space Center. If NASA HQ becomes inaccessible or as directed, essential Agency leadership personnel will utilize one or more of these sites. The contractor shall support the activation of this capability.

9.0 Other Support Tasks (Non-Core Support)

This PWS represents a comprehensive set of core requirements. Other related services may be required during the life of the contract to provide direct support to Mission Directorates and Mission Support organizations. These other services will be ordered through the indefinite delivery, indefinite quantity provisions of the contract. Several examples of task orders include the following:

- Support the investigation and deployment of state-of-the-art and leading edge technologies for the Exploration Systems Management Directorate. Support to this task has a Research and Development component that complements Headquarters core IT services by demonstrating, exploring, and exploiting new technologies within both development and production environments.

- Support the Exploration Systems Management Directorate in the planning, design, analysis, development, implementation, and training support to the Integrated Collaborative Environment (ICE) project.

- Support the Science Mission Directorate (SMD) through the enhancement of SMD business systems and processes placing emphasis on integration, collaborative solutions, knowledge management, and communications technologies. In addition, develop, maintain, and document the SMD IT architecture as it relates to the Agency IT architecture and to any locations hosting SMD servers/applications.

- Support the daily operations and strategic planning for the HQ Space Operations Center (SOC). Activities include demonstrations, training, on-site support, operation of desktop, web-based and other advanced applications and products.

- Support the Office of the Chief Financial Officer by maintaining the Central Resource Control System, NASA Audit Tracking System, CFO Web Site Portal, and Financial Management Internal Control System.

- Support the Office of Public Affairs (OPA) to include application development, IT strategic guidance, technical support and maintenance, test-bed provisioning, recommendations of software and hardware, multimedia support, and research and development support.

- Support the Chief Information Officer with expert level consultation, recommendations and support on Security Program Management, Governance and Oversight, Security Operations and Security Architecture and Engineering. In addition, provide program management support for each of the Program Managers in the OCIO, including Architecture and Integration, IT Security, Enterprise Portfolio Management, and Policy and Investment; eGovernment Initiatives support; Application Portfolio Management support throughout the Agency; and Agency Business Systems Support.

Appendix A. Data Requirements Documents DRDs

DRD #1	Documentation environment of metrics, analytics and deliverables implementation plan and migration schedule	Updated and available weekly during the first two months of contract start; enhancements and additional content added monthly thereafter until established baseline schedule is met
DRD #2	Transition plan and integrated schedule	Available at contract start with significant weekly updates for the transition period up to Operational Readiness Review and acceptance.
DRD #3	Contract Status Meeting	Monthly – no later than last week of the month
DRD #4	Daily TagUp Review	Daily
DRD #5	Integrated Master Schedule with ability to drill down to supporting data, including resource loading	Updated every 2 weeks from contract start date.
DRD #6	Project Schedule Adherence Report	Monthly – no later than second week of the month
DRD #7	Logistics Management Plan	One month after contract start date.
DRD #8	HQ Enterprise Architecture Plan Updates	240 days after contract start date
DRD #9	Operational Level Agreements	In accordance with Government schedules
DRD #10	Report on response times, ticket aging, and customer satisfaction, delivered	1 month after start date and monthly after that.
DRD #11	Root Cause Analysis and Corrective Action Plan	as requested by ITCD
DRD #12	Configuration Management Plan	Update as required by ITCD
DRD #13	CCB Meeting Minutes	Weekly – 1 day after meeting
DRD #14	Spare Parts Inventory Report	90 days after contract start, quarterly thereafter
DRD #15	Summary of updates to ROSA showing what was modified over previous 3 months	Available quarterly
DRD #16	Diagrams of Application logic, connectivity, interdependence and data flow	90 days after contract start and update continuously

DRD #17	Diagrams of Server dependencies (sinks/sources), physical placement and relationship	90 days after contract start and update continuously
DRD #18	Health & Safety Plan	Submit with proposal
DRD #19	Occupational Injuries and Illnesses Report	One month from contract start and monthly thereafter
DRD #20	Customer Service Metrics Proposal	Deliver within one month of contract start
DRD #21	Customer Satisfaction Survey Report	Deliver at contract start with the customer satisfaction survey, monthly summary analytics and trending
DRD #22	Training Program & Outreach Plan, detailing materials, methods and approach and to include communications, and facilitating relationship building activity. Initial plan and updates shall be submitted on time.	One month from contract start
DRD #23	Customer Advisory and Service Review, meeting notes, action items, results, and schedule.	As required within 2 business days of meetings.
DRD #24	Customer Requirements Adherence Metrics Proposal	Deliver within one month of contract start
DRD #25	Requirements Adherence Report	Deliver at contract start date, monthly thereafter
DRD #26	Summary and Trend Ticket Reporting including number of tickets opened, completed and pending (e.g. under a week, under two or over three) number escalated, rating, closed, times to first respond, customer satisfaction	One month from contract start date and monthly thereafter
DRD #27	Service Request Processing Plan describing overall management and execution of the SR system and customer satisfaction report	Within two weeks of contract start date
DRD #28	Customer Satisfaction Summary and Trending Report	One month after contract start date, monthly thereafter
DRD #29	Catalog Orders Report includes number of orders by category, number complete, funds used versus available, funds in process	Two weeks from contract start date, monthly thereafter
DRD #30	Application Service Framework	Two weeks from contract start date, modifications reflecting approved changes as required
DRD #31	Application Service Roadmap and Implementation Plan	Three months after contract start and every six months thereafter, modifications reflecting approved changes as required.
DRD	Legacy application disposition plan	Six months from contract start

DRD #32	Legacy application disposition plan	Six months from contract start date, modifications reflecting status and approved changes every 60 days
DRD #33	Legacy application migration report	Six months from contract start date, modifications reflecting status and approved changes every 60 days
DRD #34	Framework for Development Program	Due at contract start, modifications reflecting approved changes as required
DRD #35	Interface Control Documents	One month from contract start date
DRD #36	Software Management Guide	Three months after contract start date, modifications reflecting approved modifications quarterly thereafter
DRD #37	Standard requirements template that documents the service or design need from the perspective of effected discipline areas (e.g. applications development, IT security, customer training, operations) and by level of need (e.g. mandatory, optional, preferred).	Within two months from contract start date
DRD #38	System Design Specification	Two months from contract start date, modifications reflecting approved modifications as needed thereafter
DRD #39	Application Status Review materials	One month from contract start, monthly thereafter
DRD #40	Portfolio Management Views of Application Services and Inventories	Six months from contract start date, continuously thereafter
DRD #41	As built detailed functional and physical description of development environment, its interfaces and processes	Two months from contract start date, provided within 2 days of changes to structural or ITS environment including patches
DRD #42	Application & Website delivery implementation plan	Two months from contract start date
DRD #43	Version Description Document	Scheduled in accordance with CCB
DRD #44	Application & Website delivery	Two months from contract start date, available continuously thereafter
DRD #45	Data Exchange Agreement diagram, performance and exception report	One month from contract start date and monthly thereafter
DRD	Service Level Agreement performance and exception	One month from contract start

DRD #47	Availability of hosted and housed services	One month from contract start date and monthly thereafter
DRD #48	Performance of hosted and housed services	One month from contract start date and monthly thereafter
DRD #49	Diagram of server location	Three months from contract start date and on-demand thereafter
DRD #50	Diagram of servers logical connection to network	Three months from contract start date and on-demand thereafter
DRD #51	Capacity and Performance Report	Two months from contract start date, on-demand thereafter
DRD #52	Quarterly/Monthly Patch Release Report	One month after contract start date, monthly thereafter
DRD #53	Equipment Upgrade Evaluation Report	90 days of contract start date and semiannually thereafter
DRD #54	Intrusion Detection Summary	One month after contract start, monthly thereafter
DRD #55	Data Center System Assessment & Recommendations Report	90 days from contract start date, monthly thereafter
DRD #56	Online Innovation Environment. Provide updates, align content so that it is searchable and at the accepted level of detail.	90 days from contract start date, monthly thereafter
DRD #57	Data Center Modernization Plan	Two months from contract start date, and every six months thereafter
DRD #58	HQ Tactical Plan	Annual and updates as required
DRD #59	Systems Engineering & Integration Test Lab Performance Report	Two months from contract start date, continuously available thereafter
DRD #60	Contractor Information Security Management Plan	Within one month from contract start date, updated annually thereafter
DRD #61	Draft Policy, Requirement, Procedure, or Standard	In accordance with accepted SOP updates
DRD #62	eMail Data Search Results	On demand
DRD #63	Monthly Privileged Position Report	Within one month from contract start date, monthly thereafter
DRD #64	Security Reviews and Assessments	On demand
DRD	Daily Risk Vulnerability Report	daily

DRD #65	Daily Risk Vulnerability Report	daily
DRD #66	Monthly Vulnerability Scan Report (encrypted)	One month after contract start date, monthly thereafter
DRD #67	Monthly Analog Telephone Scanning Report (encrypted)	Two months after contract start date, monthly thereafter
DRD #68	Monthly Wireless 802.11 Scanning Report (encrypted)	Two months after contract start date, monthly thereafter
DRD #69	Annual Penetration Test Plan and Rules of Engagement and Schedule	annually by fiscal year's end
DRD #70	Annual HQ Penetration Testing Report	annually by fiscal year's end
DRD #71	IT C&A Security Plan Assessment using the NASA standard template	annually by fiscal year's end
DRD #72	Risk Assessment	annually by fiscal year's end
DRD #73	Security Controls Assessment Report Assessment using the NASA standard template	annually by fiscal year's end
DRD #74	Plan of Actions and Milestones Assessment using the NASA standard template	annually by fiscal year's end
DRD #75	System Certification Report	annually by fiscal year's end
DRD #76	Monthly POA&M Status Report	One month after contract start date, monthly thereafter
DRD #77	Monthly ISSA Status Report	Two months after contract start date, monthly thereafter
DRD #78	Incident Response Training and Test Report	annually by fiscal year's end
DRD #79	Quarterly Metric Report summarizing the transaction history, incidents, and inventories/inspections for that	Due 90 days from contract start date, and every 3 months